Electronic Research Administration
A program of the National Institutes of Health
National Institutes of Health
Office of Extramural Research

# Account Management Module (AMM) User Guide for Commons Users

August 4, 2023

**NOTE:** This user guide is an identical PDF version of the online help.

# Contact Us

**Additional Help Needed?** Please contact the eRA Service Desk (https://www.era.nih.gov/need-help).

**Toll-free:** 1-866-504-9552; **Phone:** 301-402-7469

**Hours:** Mon-Fri, 7:00 a.m. to 8:00 p.m. Eastern Time

**Feedback on the user guide?** Please email the eRA Communications Office (era-communications@mail.nih.gov).

# Disclaimer STATEMENT

No data shown in illustrations represents any real account, project, or individual. Any resemblance to actual accounts, projects, or individuals is purely coincidental.

# Latest Updates

Updates and new features in AMM:

**July 27, 2023**

**New Look and Feel for Online Help and User Guide**

- The online help and user guide have been updated to the new look and feel, consistent with the new look and feel of eRA Modules. There are no changes to the function of the help topics.

**New Name for AMM**

- Account Management has been rebranded as Account Management Module (AMM) to distinguish it from the HHS Access Management System (AMS), and the online help has been updated to reflect this change.

# Overview

The Account Management Module (AMM) facilitates user and system account administration based on assigned user roles. The system provides the ability to search existing accounts. When a search is performed, all records that meet the search criteria are returned on the *Search Accounts* screen.

## Commons Management Staff

Once the institutional account is created, the Signing Official (SO) at each grantee organization is able to establish additional user accounts with various levels of access and capability. The SO or Accounts Administrator (AA) may then create additional accounts for the administrative and scientific staff.

SOs only can also view, create, and maintain system accounts.

## User Roles

The following users have the ability to search for, manage and create accounts, and to add or remove roles for user and system accounts:

### Commons Management Staff

- Accounts Administrator (AA)
- Administrative Official (AO)
- Business Official (BO)
- Signing Official (SO)

## Account Statuses

AMM user accounts can have the following statuses:

- Active — A valid account in good standing.
- *Deactivated* — Account has been disabled by an administrator
- *Locked due to inactivity* — Locked by the system due to inactivity (no user activity for 120 days).

- *Pending Affiliation* — Account has not yet been associated to an organization
- *Profile Only* — A profile that is not associated to a user account.

# Accessing AMM

## Users Who Create and Manage eRA Commons Accounts

1. After logging into Commons, access AMM from the Commons welcome screen by clicking the **Account Management (Admin)** tile, or selecting **Admin** from the *Apps* menu.
2. When you take one of these actions, the AMM *Search Accounts* screen opens.

For instructions on performing a search, see Search Account.

**NOTE:** If you see an eRA/IMPACII Systems Rules of Behavior page, you must read it over and agree to terms before you are allowed to access IMPACII modules. See eRA/IMPAC II Rules of Behavior Agreement for more information.

# Account Search

Use the *Search Accounts* screen to search for existing account(s) within or outside of your organization or institution.

See Search for Accounts

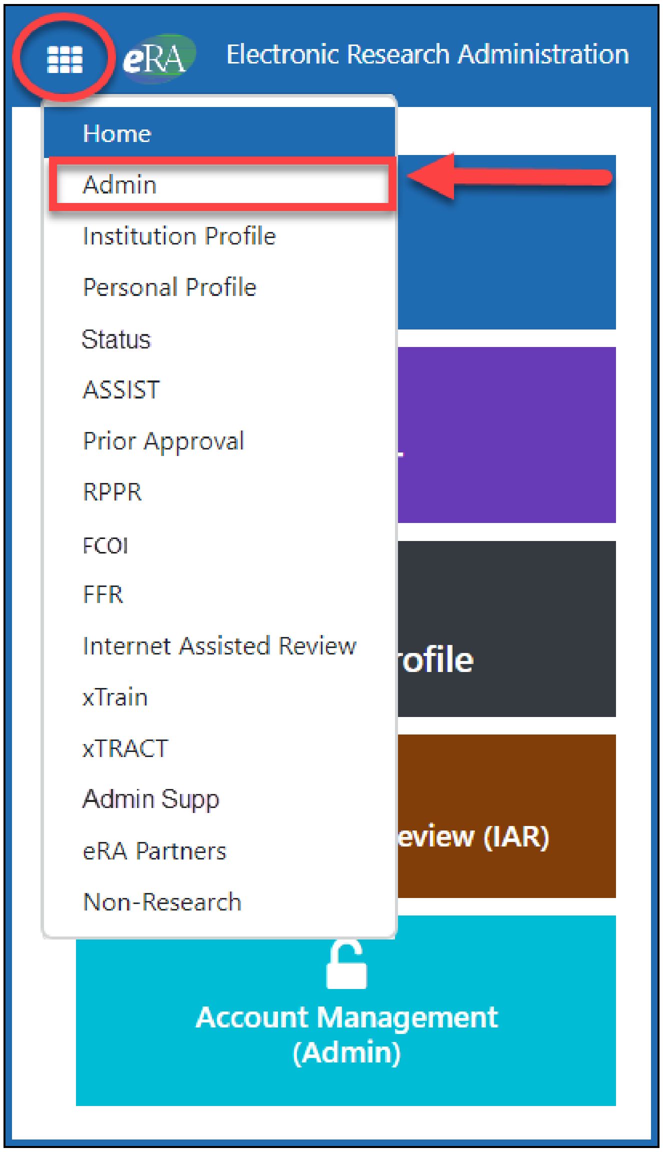
### Certificates

For information on obtaining and registering a certificate from a Certificate Provider or Authority, please refer to the Web Services Certificate (S2S) Guide:Section 2.4.3 for Commons users

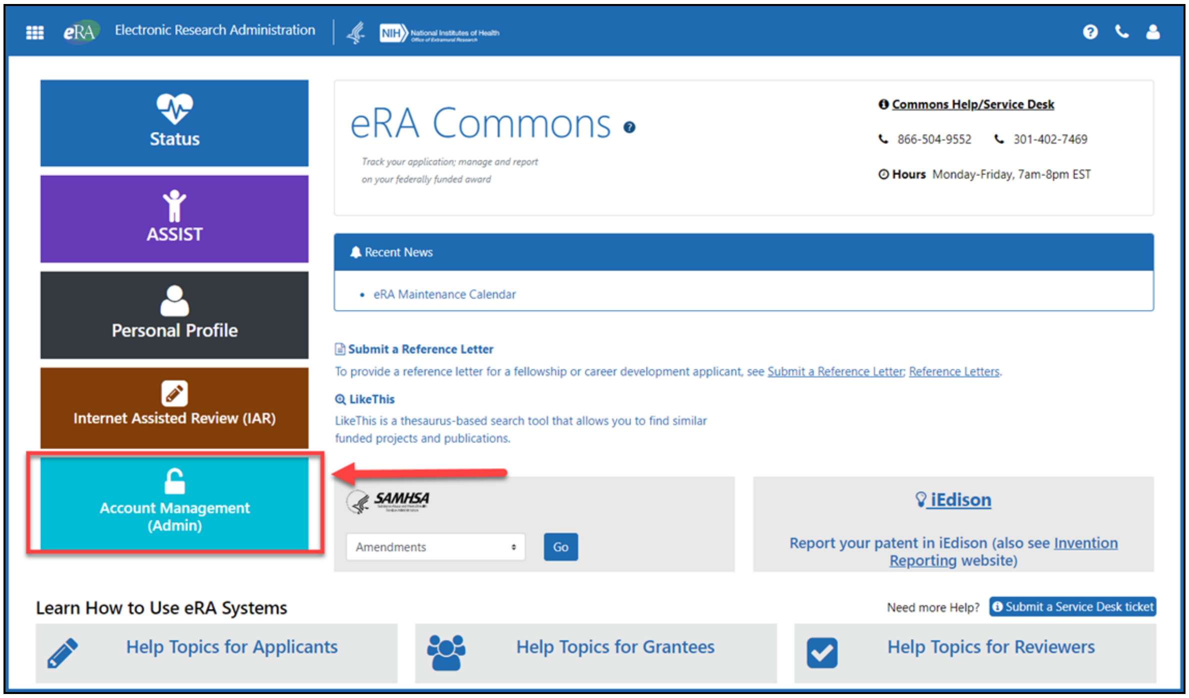
## Search for Commons User Accounts

### Accessing Search

1. After logging into eRA Commons, the signing official or other authorized users can access the Account Management Module by selecting **Admin** from the apps icon in the upper left corner, as shown here:




1. Or by clicking the **Account Management (Admin)** button on the eRA Commons landing page, as shown here:




2. Clicking either **Account Management (Admin)** button opens the AMM *Search Accounts* screen described below.

From there, they can select the **Manage Accounts** sub-menu.

## The Search Accounts screen

Clicking on **Account Management (Admin)** opens the AMM *Search Account* screen shown below.

The *Search Accounts* screen for external users provides the ability to search for existing user and system account(s):

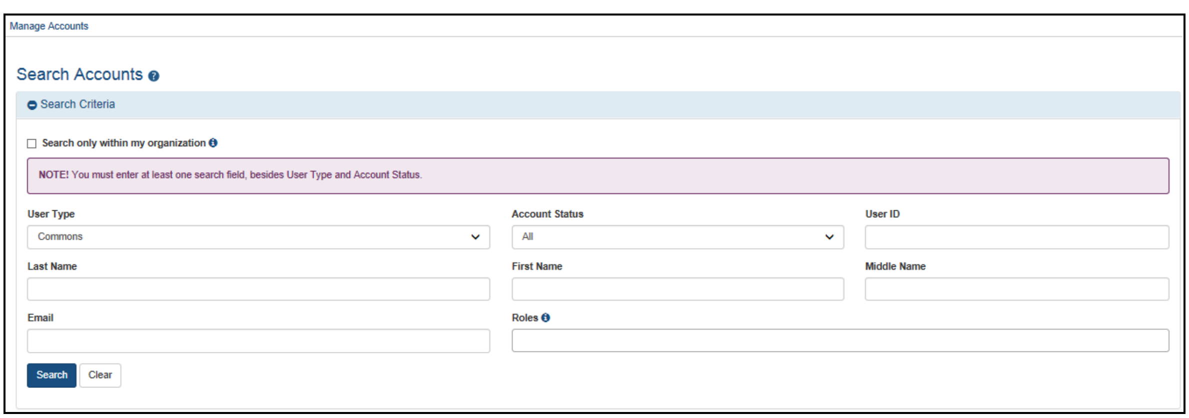


*Figure 1: Search Accounts Screen for External Users*

**NOTE:** You must enter at least one search field, besides the **User Type** and **Account Status**.
Wild card characters such as the percent sign (%) can be used to search for a string of characters.

To Search:

1. Enter the appropriate search criteria in at least one of the other search fields.
2. Click the **Search** button to execute the search or click **Clear** to clear the search criteria.
3. The system returns the search results. For more information see Commons User Account Search Results.

**NOTE:** Use the **User ID** field to search by IMPACII user ID

## Search Options

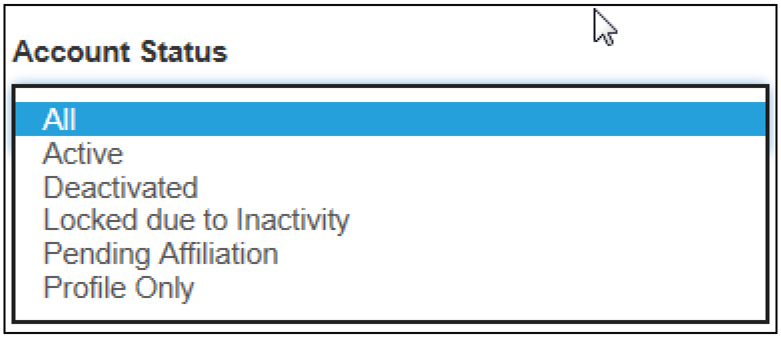
### Search by Role

To search by role, select a role from the Roles drop-down menu (to select multiple roles, hold the **<Ctrl>** key as you click the roles).

**NOTE:** When you search by roles, you can only search within your organization. You can select multiple roles, but the default search is for all roles appropriate to the logged in user's account role.

### Search by Status

You can search by status to locate accounts that have been deactivated (by an administrator or due to inactivity). To do so, select the appropriate status from the **Account Status** drop-down menu:




Make your selection and click **Search** to proceed.

### About Locked Accounts

The status *Deactivated* indicates that the account has been disabled by an administrator, while the status *Locked due to inactivity* is applied to accounts that have had no activity for 120 days.

For information on reactivating a deactivated account, see [Reactivate or Unlock Account.]

## Commons User Account Search Results

When you click the **Search** button, the **Search Results** display below the Search Criteria on the *Search Accounts* screen:

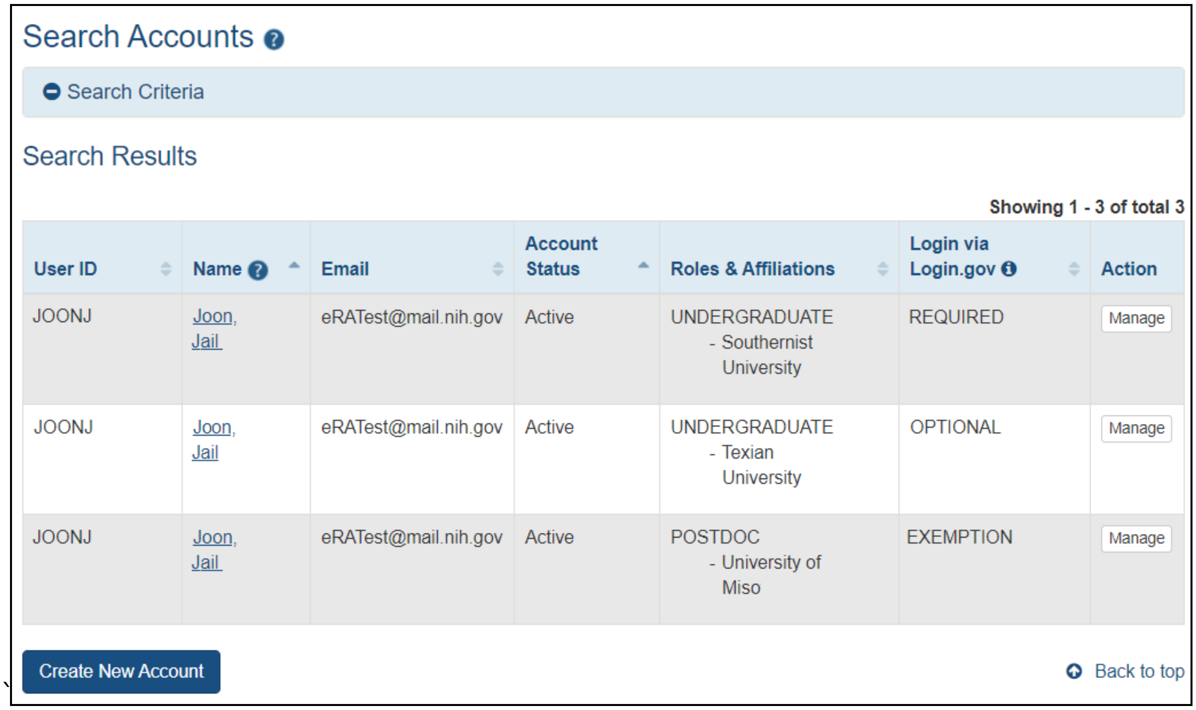



*Figure 2: Commons User Account Search Results*

**NOTE:** The **Create New Account** button does not display until a search is performed.

### Working with the Search Results

- **User ID**
- **Name** - last name, first name
- **Email**
- **Account Status** -
  - *Active* - The **Manage** button displays in the **Action** column.
  - *Pending* - The **Resend Email** button displays in the **Action** column.
  - *Pending Affiliation* - The **Manage** button displays in the **Action** column.
  - *Profile Only* - The **Create** button displays in the **Action** column.
- **Roles & Affiliations**
- **Login via Login.gov**
- **Action** - The **Action** buttons are **Manage**, **Resend Email**, and **Create**.

Perform one or more of the following steps

1. To view the **Search Criteria**, click anywhere in the **Search Criteria** bar.
2. To filter the search results, enter the appropriate value in the **Filter Results:** text box and hit the **<Enter>** key.
    a. For example, to view all users with the Internet Assisted Review (IAR) role, type *IAR* in the **Filter Results:** text box.

**NOTE:** The default number of records per page is 10.

3. To change the number of records per page, select the appropriate number in the **Show per page** column.
4. To navigate between pages, perform one of the following options:
    a. Click the appropriate **Page Number** button.
    b. Click the **right double arrows** button to go to the end of the list.
    c. Click the **left double arrows** button to go to the beginning of the list.
5. To sort the search results, click the click the appropriate column heading name's **down arrow** (ascending sort) or the **up arrow** (descending sort). The default sort is by **Name** (Last Name, First Name).
6. To view the *NIH Support View* screen, select the appropriate name hyperlink in the **Name** column.
    a. For more information, please see the NIH Support View topic.
7. If displayed, click the **Read More** hyperlink in the **Roles and Affiliations** column to view a Principal Investigator's (PI) multiple affiliations.
8. To return to the top of the screen, click the **Back to top** hyperlink.

### Action Options

- **Create Account**

    - To create a new account and profile, click the **Create New Account** button at the bottom of the screen, or find the correct User ID and click the **Create** button.

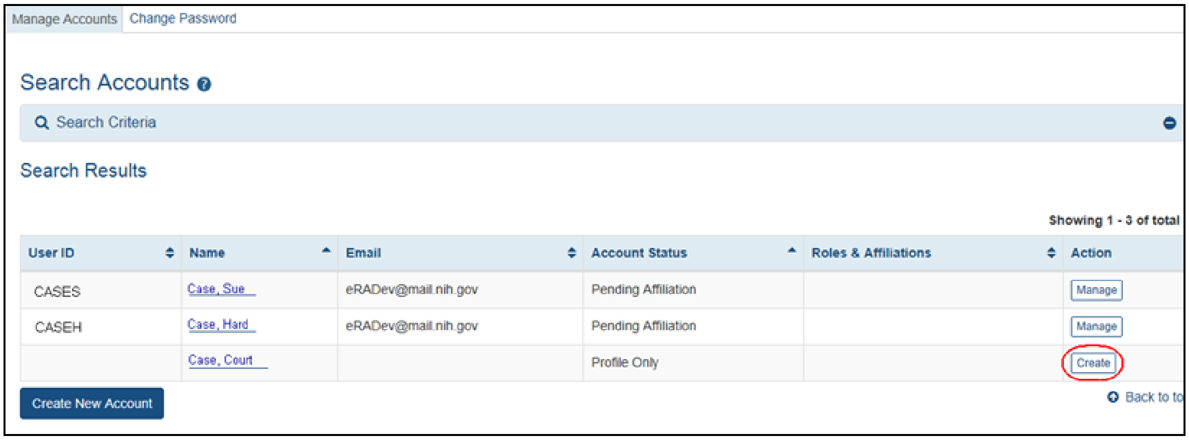



*Figure 3: Search Results showing Create button*

- Refer to the [Create Commons User Accounts] topic for more information.

- **Manage Account**

- The **Manage** button appears if the account status is *Active* or *Pending Affiliation*.

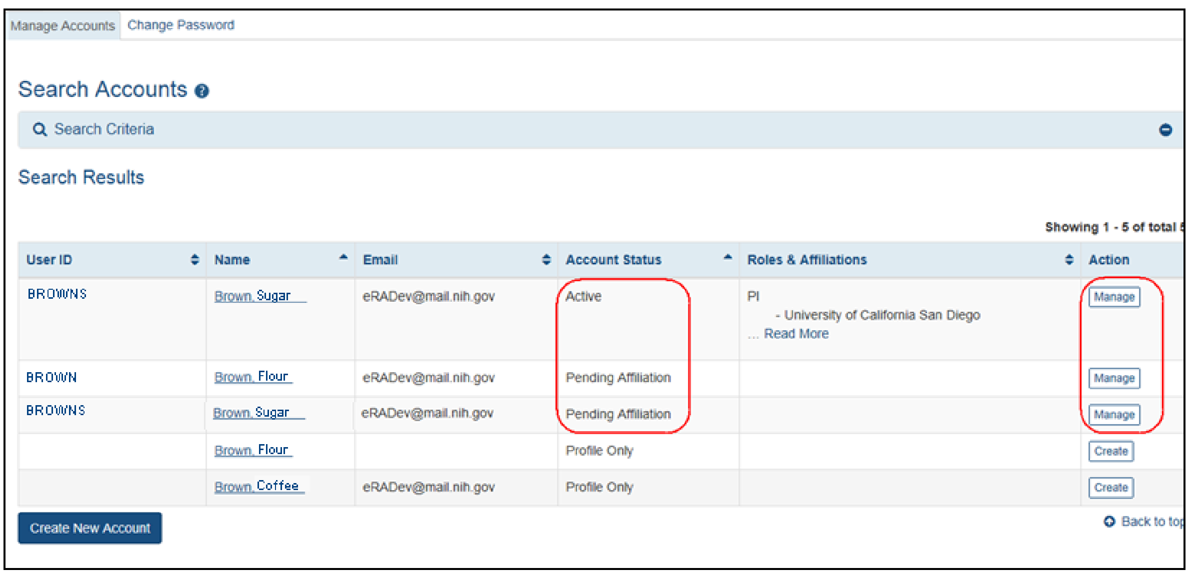



*Figure 4: Search Accounts screen with Manage button*

- To edit an account, click the **Manage** button and the Manage Account screen displays.

- Refer to the [Manage External User Accounts] topic for more information.

- **Resend Email**

- The **Resend Email** button appears on the *Search Accounts* screen for accounts that are pending user review, indicating that the user has not validated the account request.
- Click **Resend Email** to resend the account confirmation email.

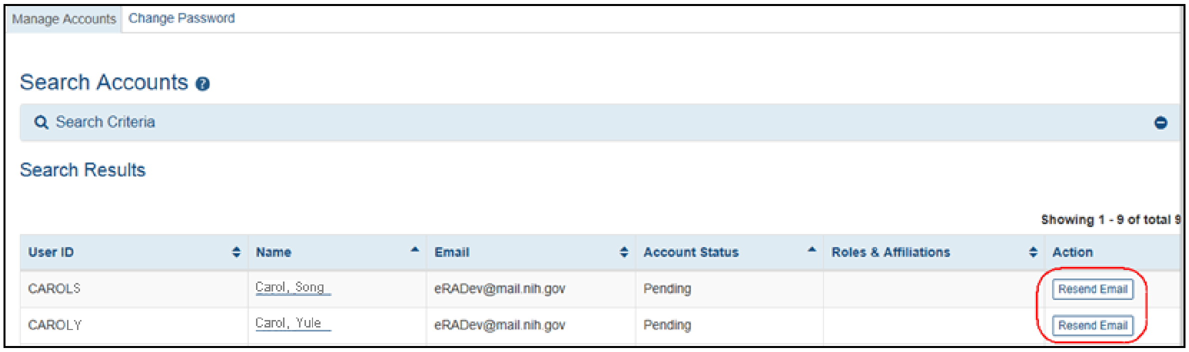



*Figure 5: Search Accounts Screen Displaying the Resend Email Button*

## NIH Funding Support View

The *Funding Support* screen lists the NIH application information associated with the selected Principal Investigator (PI). Use this information to positively identify PIs associated with your institution.

**NOTE:** The *Funding Support* screen is for Commons users only.

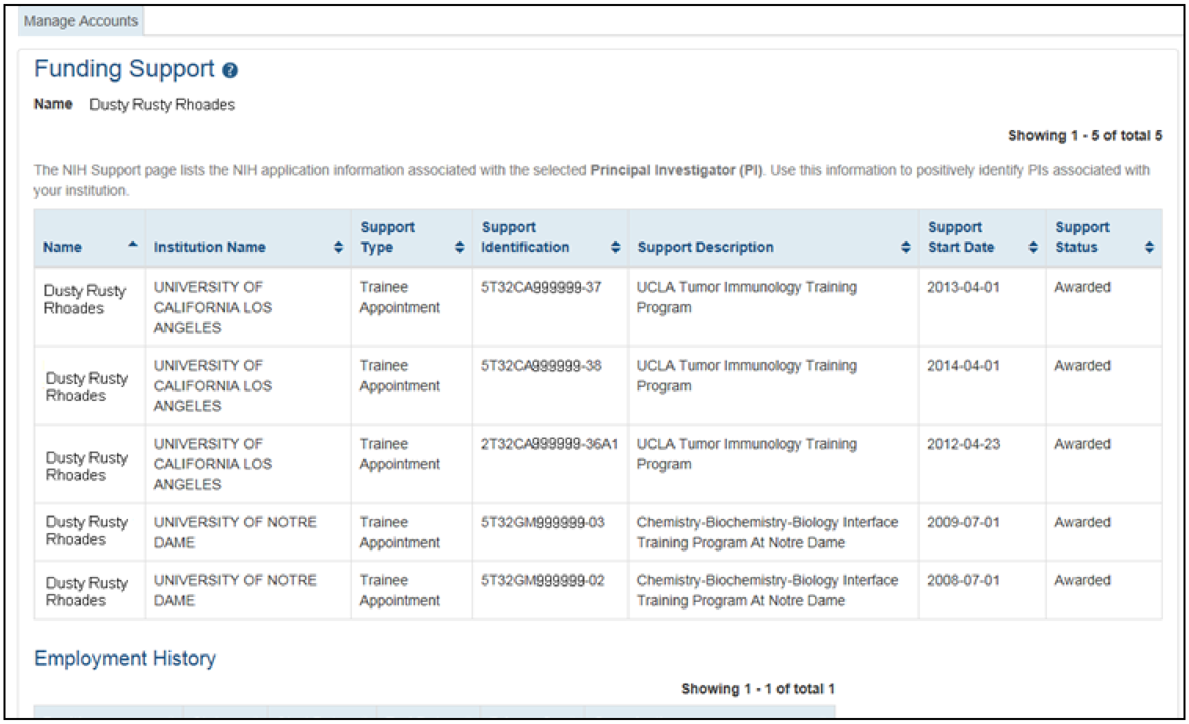



*Figure 6: Funding Support Screen*

## Search for System Accounts

Use the , to search for existing user and system account(s).

**NOTE:** Agency and Commons, users can search for and create system accounts.

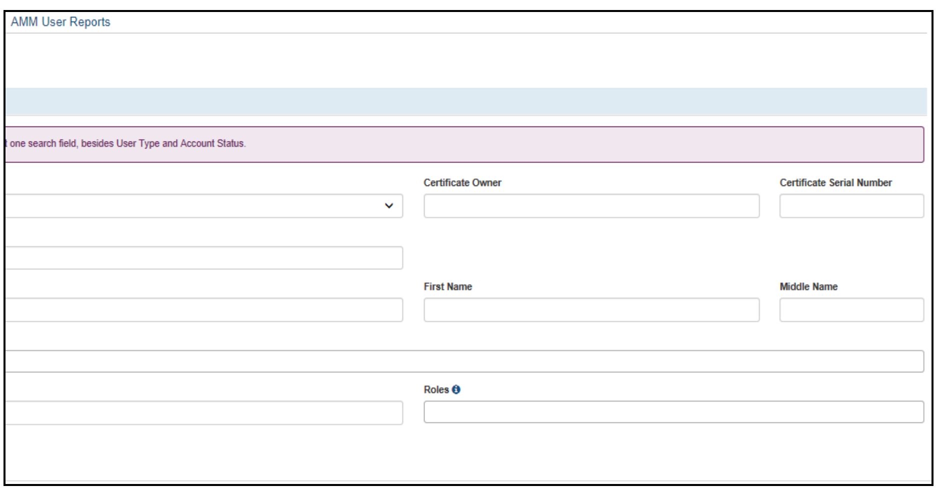



*Figure 7: Search Accounts Screen Displaying Searching for System Accounts*

**NOTE:** You must enter at least one search field, besides the **User Type** and **Account Status**.
Wild card characters such as the percent sign (%) can be used to search for a string of characters.

Perform the following steps:

1. To search for a system account, select *System* from the **User Type** field's drop-down menu.
2. Enter the appropriate search criteria in at least one of the other search fields besides **User Type**.
3. Use the **User ID** field to search by IMPACII user ID
4. If you wish, select a **Role** from the drop-down menu. (To select multiple roles, hold the **<Crtl>** key and highlight the desired roles.)

**NOTE:** When you search by system roles, you can only search within your organization. You can select multiple roles, but the default search is for all roles appropriate to the logged in user's account role.

5. Click **Search** to execute the search or click **Clear** to clear the fields and start over.

## System Account Search Results

When the **Search** button is clicked, the system displays appropriate system accounts in the **Search Results** located below the *Search Criteria* section on the *Search Accounts* screen. The search results are sorted alphabetically first by last name, first name in the **Name** field and then by **Account Status**.

**NOTE:** The **Create New Account** button does not display until a search is performed.

The following columns appear in the search results:

- **User ID**
- **Name** - last name, first name
- **Organization**

- **Roles & Affiliations**
- **Certification Owner** - The **Certificate Owner** is the organization who acquired the certificate.
- **Action** - Option button is **Manage**.

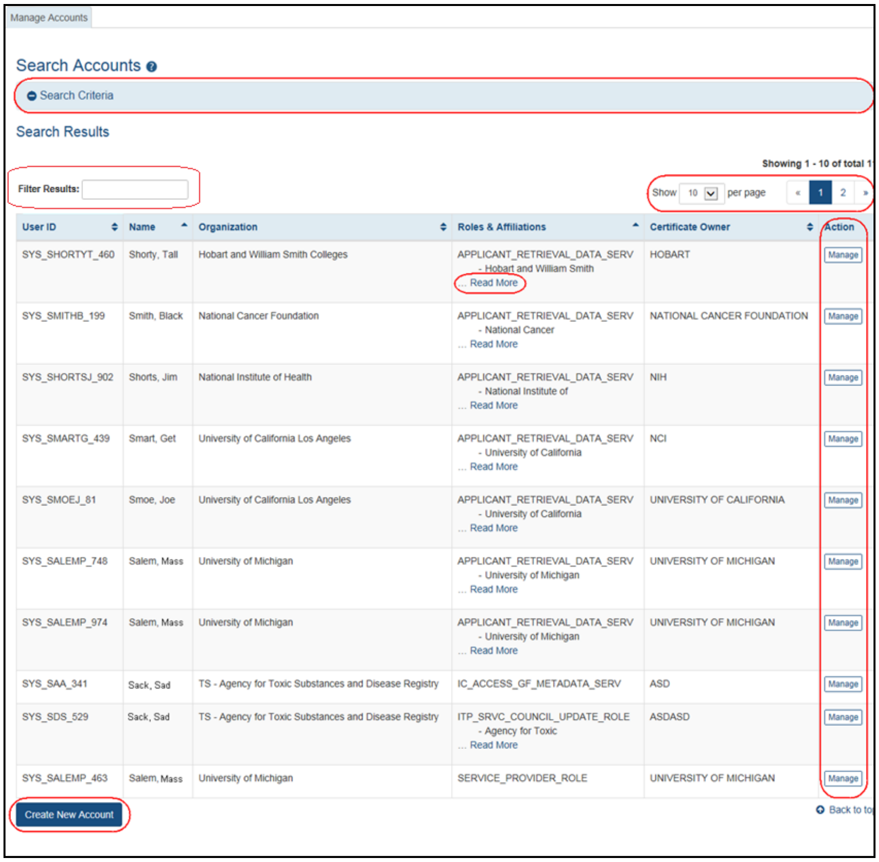



*Figure 8: Search Accounts Screen Displaying System Accounts Search Results*

Perform one or more of the following steps :

1. To view the **Search Criteria**, click anywhere in the **Search Criteria** bar.
2. To filter the search results, enter the appropriate value in the **Filter:** text box and hit the **<Enter>** key.
    a. For example, to view all users with the last name of Salem, type *Salem* in the **Filter:** text box.

**NOTE:** The default number of records per page is 10.

5. To change the number of records per page, select the appropriate number in the **Show per page** column.
6. To navigate between pages, perform one of the following options:
   a. Click the appropriate **Page Number** button.
   b. Click the **right double arrows** button to go to the end of the list.
   c. Click the **left double arrows** button to go to the beginning of the list.
7. If displayed, click the **Read More** hyperlink in the **Roles and Affiliations** column to view a system user's multiple affiliations.
8. To manage a system account, click the **Manage** button in the **Action** column.
   a. Please refer to the Manage System Accounts topic for more information.
9. To create a new account and profile click the **Create New Account** button at the bottom of the screen.
   a. Please refer to the Create System Account topic for more information.
10. To return to the top of the screen, click the **Back to top** hyperlink.

# Create Accounts

You can create the following types of accounts:

## Create User Accounts

## Create System Accounts

## Create Commons Account

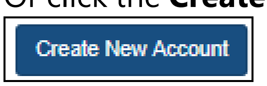
If you are a Commons user with an SO, AA or BO role, you have the ability to create new Commons user accounts (such as for a PD/PI).

---

**IMPORTANT:** PD/PIs cannot create their own accounts: Only an SO or AA Commons user can create this account.

---

1. To create a new user account, first search AMM to make sure the user doesn't already have an account. For instructions, seeSearch Account for Commons Accounts
2. You launch the create-account process from the Search Results screen Search Results screen.
   - In the search results, profiles that are not already associated to a user account display a **Create** button in the Action column: 


     Click the **Create** button to create a user account for that profile.
   - Or click the **Create New Account** button located below the search results:
     

3. When you click one of the **Create** buttons, the *Create Account* screen opens, as shown below.

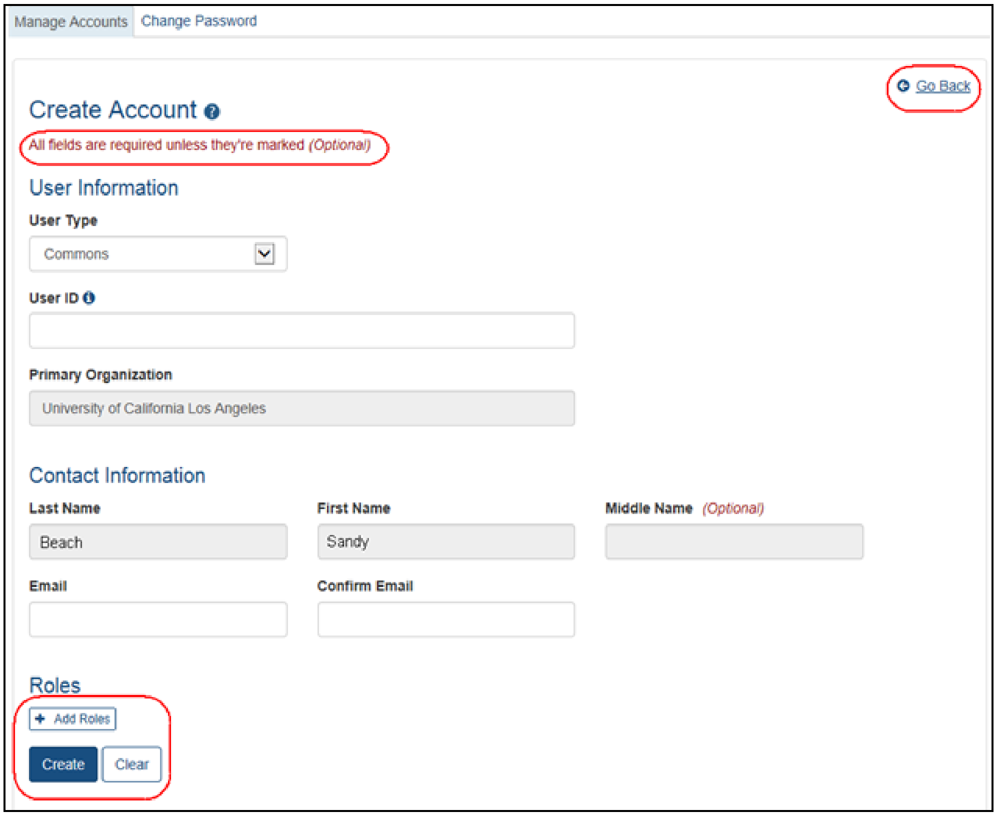



*Figure 9: Create Account Screen for an External Account*

Perform the following steps to create an account:

4. Set **User Type** to Commons.
5. Enter the **User ID** or let the system generate one.
    a. The **User ID** length should be between 6 and 30 characters and should **NOT** contain special characters except the @ sign, the hyphen, the period, and the underscore.
    b. The system can display the following messages: This User ID is available OR This User ID is already taken, please use another one.
6. Usually the **Primary Organization** defaults to the logged in user's organization.
    a. If there is no user organization name selected, click the magnifying glass icon to assign a **Primary Organization**. (See Set Primary Organization for more information.)

7. Perform one of the following options:
    a. When the account information is complete, click **Create** to create the account or click **Clear** to clear all information from the form.

When you click **Create**, the system displays the *Account Details* screen with a success message, as shown here.

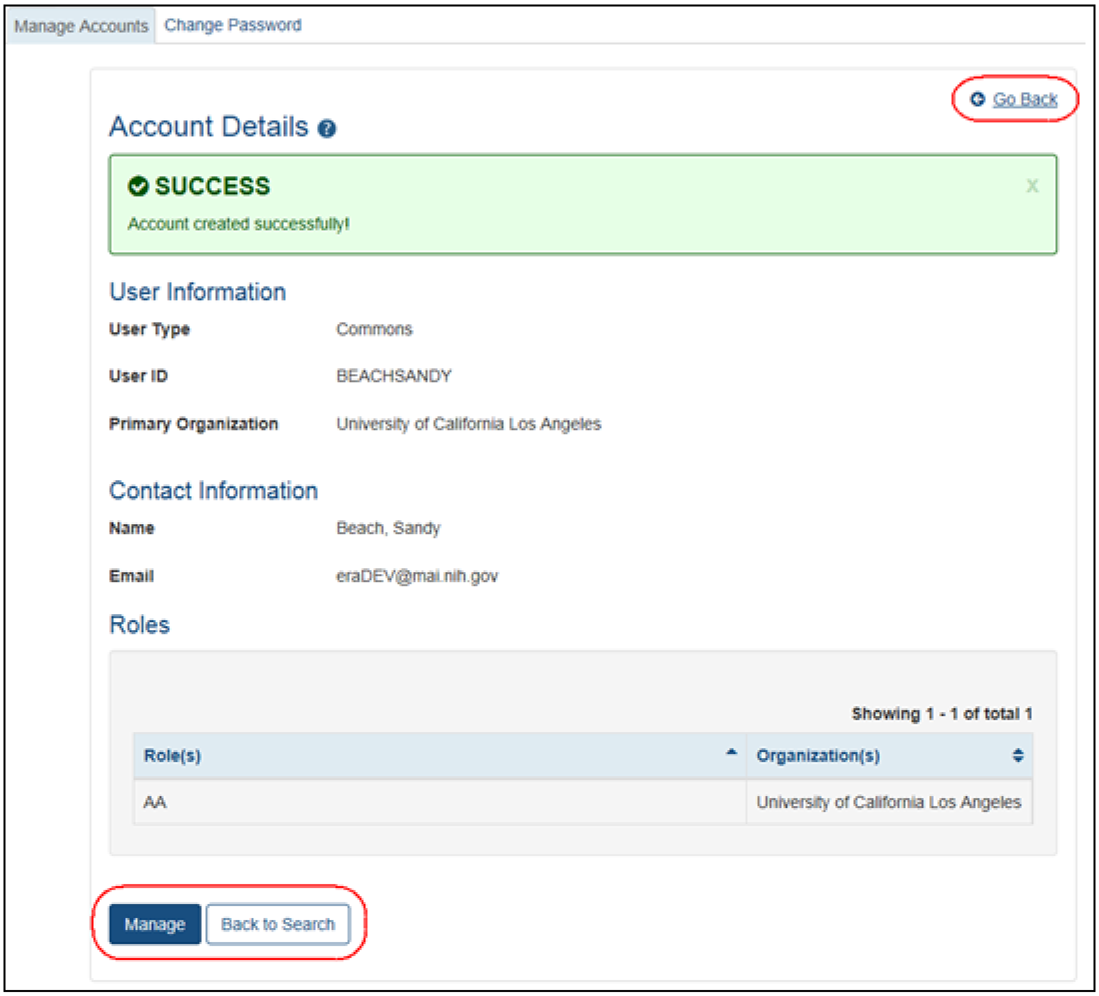



*Figure 10: Account Details Screen with success Message*

6. Perform one of the following options on the *Account Details* screen:
    a. To return to the *Search Accounts* screen displaying the previous search results, click the **Go Back** hyperlink.

b. To edit the account's information, click the **Manage** button.
    i. For more information, please refer to the Manage Account for Commons Users topic.
c. To return to the *Search Accounts* screen to enter new search criteria, click the **Back to Search** button.

## Account Invitations from eRA Systems

Create-Account requests for eRA accounts that are validated by invitations from eRA modules can be approved or rejected automatically:

- If the identifying information the new user submits unambiguously matches the profile created by the account requester and the profile is not already associated to another user account, the request is approved automatically.
- If the identifying information is incorrect or an account already exists for the user profile, or if a comment has been entered in the user's funding and committee service history, request is denied and the system sends notifications to the account requester and to the eRA Service Desk.

### Examples of system-generated account invitations:

- **SO creates a new PI account in AMM**

  The new PI receives a system-generated invitation to log in to eRA Commons and validate the account.

- **SRO enables a new reviewer in Internet Assisted Review (IAR)**

  The reviewer receives a system-generated invitation to log in to eRA Commons and create an account to access IAR. See the IAR Online Help for information on enabling reviewers

- **PD/PI appoints a new trainee in xTrain**

  The trainee receives a system-generated invitation to log in to eRA Commons and create an account to access xTrain. See xTrain Online Help for information on appointing trainees.

### Workflow

The account invitation procedure includes these steps:

1. The account requester creates the new account.
2. The new user receives an email notification that includes the username and other details about the new account.
3. The user receives a second email that includes a temporary password for the new account and instructions for logging into the system. This email explains that that the user must login to the system that day or the account will be locked. After an account is locked, any attempt to log in will be redirected to the password reset/lost password workflow.. See Initial Login to eRA Account.
4. The user logs in with the provided credentials and is immediately instructed to create a new password for the account.

**NOTE:** If the user enters incorrect login information too many times, the account is locked and the user must contact the eRA Service Desk to complete the login process.

## Add/Delete User Roles

**Agency-Specific Instructions:** State Department users only - For information on adding countries, please refer to the Add/Delete Countries topic.

**NOTE:**
1. The list of roles displayed is dependent on the logged in user's role.
2. Accounts with scientific roles should be maintained for the career of the scientist, and affiliations should be added as necessary.
3. Administrative roles cannot be combined with scientific roles on the same user account, and accounts with administrative roles cannot be affiliated with more than one institution.

1. To add user roles to an account, click on the **+ Add Roles** button at the bottom of the *Create Accounts* or *Manage Accounts* screen.


When you click **+ Add Roles**, the *Add Roles* screen opens.

**NOTE:** If you click **+ Add Roles to other org**, the Manage Account window opens first, so you can search for and select the other organization.


Select the organization and click **Next** to proceed to the *Add Roles* screen as described below.

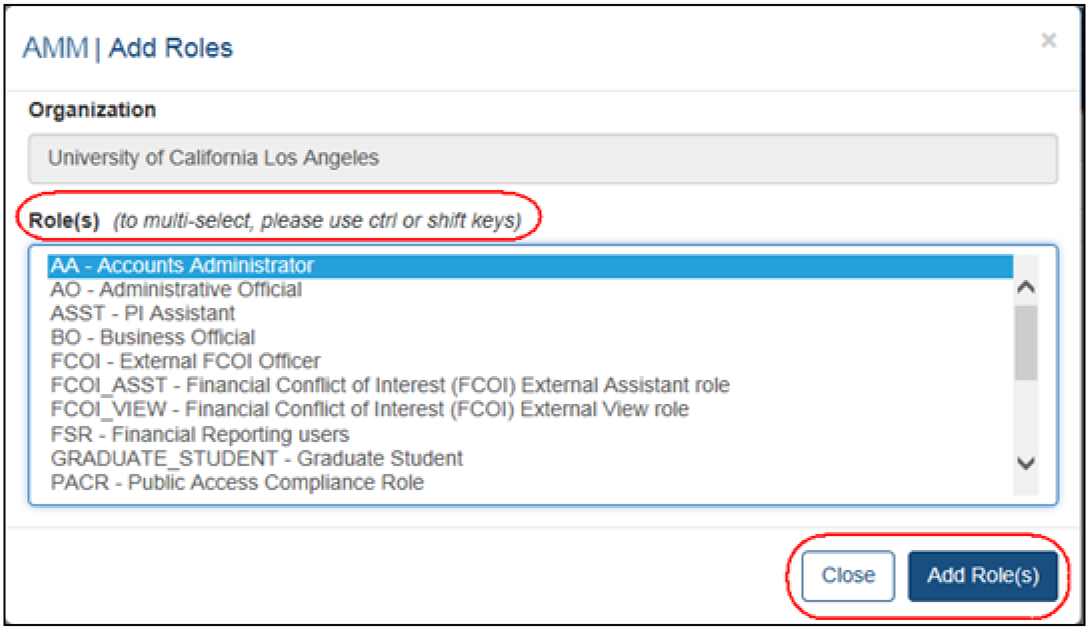



*Figure 11: Add Roles screen*

1. Scroll through the list and click to select the appropriate role(s).

   **Note**: For reference, here is a [complete list of Commons user roles](#).
2. Click the **Add Role(s)** button.

When you click **Add Roles(s)**, the system returns to the *Create Account* or *Manage Account* screen and displays the newly added role(s) .

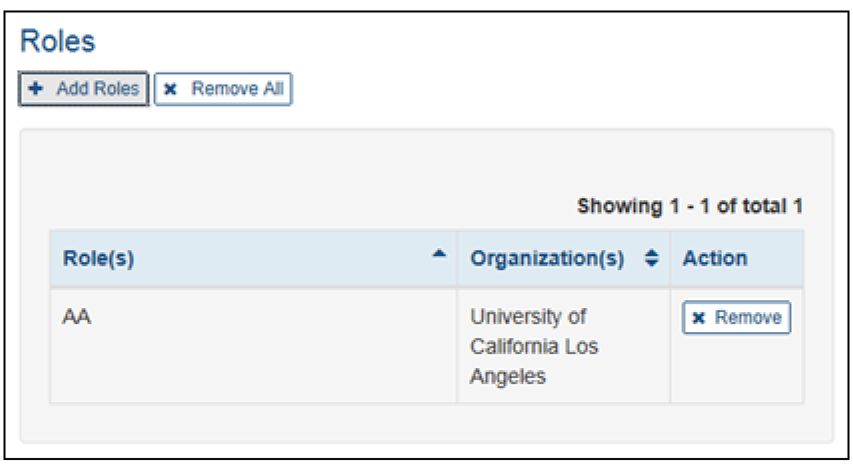



*Figure 12: Roles Section on the Create Accounts Screen*

3. To add additional roles, click the **+ Add Roles(s)** button and repeat the steps above.
4. To remove a role, click the appropriate **Remove** button in the **Action** column.
5. To remove all roles, click the **Remove All** button.

**NOTE:** You cannot remove Signing Official (SO) role when the Research Performance Progress Report (RPPR) is assigned.

**NOTE:** You cannot add user a role if the account is in deactivated status: You must reactivate the account first.

## Set Primary Organization

**NOTE:** The **magnifying glass** for the **Primary Organization** field on the *Create Account* screen appears if the logged in user is not affiliated with an Organization, IC, or Agency. Usually the **Primary Organization** defaults to the logged in user's Organization.

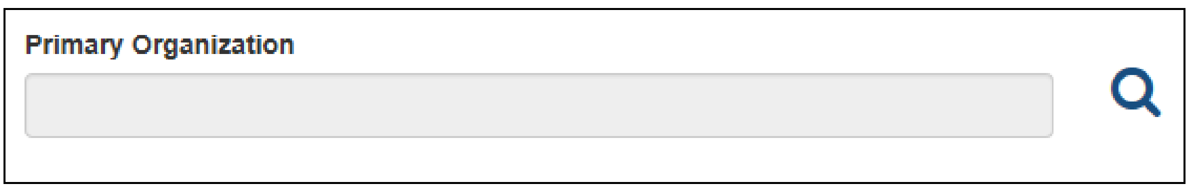



*Figure 13: Primary Organization Field*

1. To add a primary organization click the **magnifying glass** icon on the *Create Account* screen.

When the **magnifying glass** icon is clicked, the *Search Organization and Add Roles* screen opens.

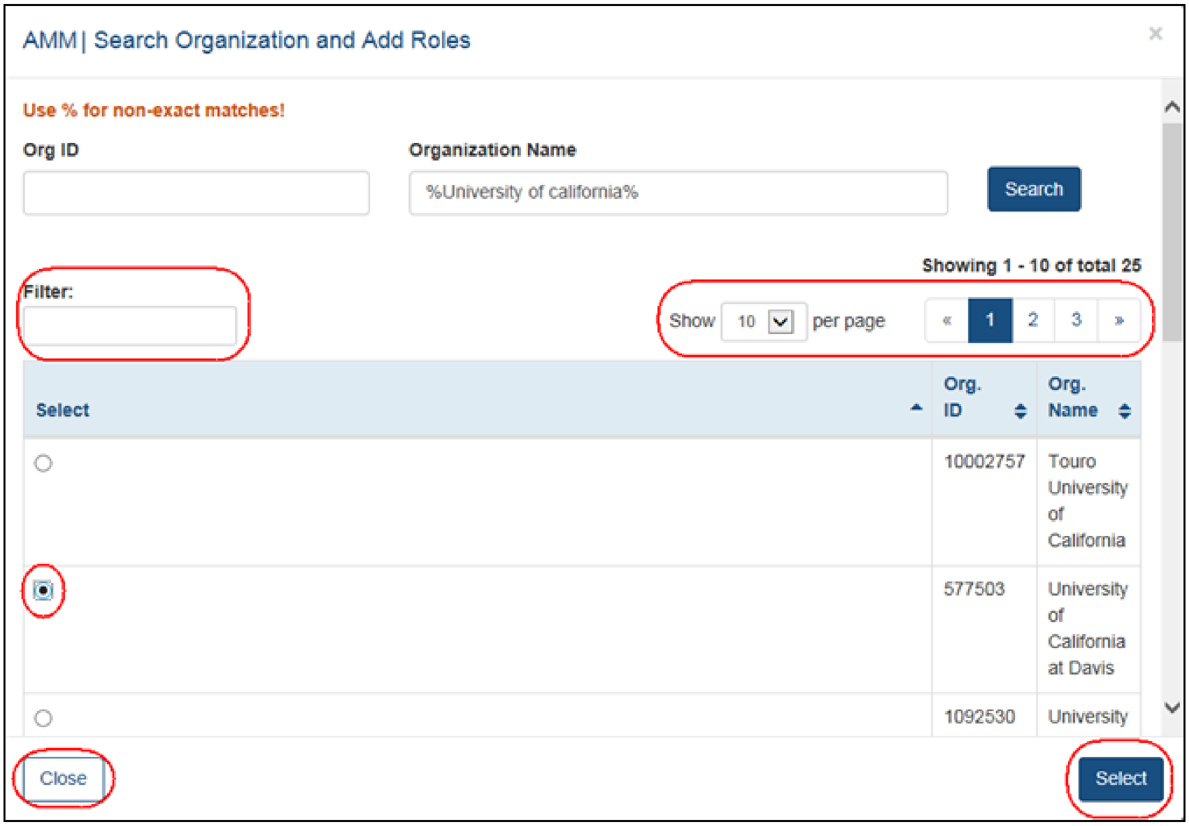



*Figure 14: Search Organization and Add Roles Screen*

2. Enter an **Org ID** or an **Organization Name**.

**NOTE:** Wild card characters such as the percent sign (%) can be used to search for a string of characters.

3. Click the first **Search** button.

When the first **Search** button is clicked, the organization is displayed, if present.

4. To filter the search results, enter the appropriate value in the **Filter:** text box and hit the **<Enter>** key. For example, enter *San Diego* to view only those universities in California.
5. To change the number of records per page, select the appropriate number in the **Show per page** column.

6. To navigate between pages, perform one of the following options:
    a. Click the appropriate **Page Number** button.
    b. Click the **right double arrows** button to go to the end of the list.
    c. Click the **left double arrows** button to go to the beginning of the list.
7. Select the appropriate organization's radio button.
8. Click the second **Select** button or click the **Close** button to close the screen.

When the second **Select** button is clicked, the *Create Account* screen displays the selected primary organization. For more information see Create External User Accounts.

## Create System Accounts

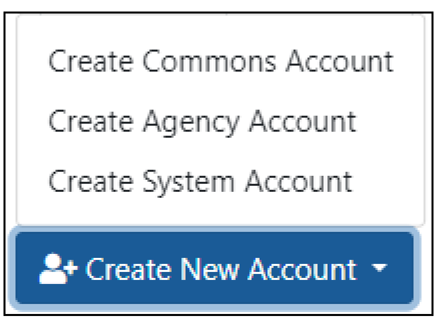
System accounts are used to access eRA Web Services.

Agency and Commons, users can create system accounts.

1. To create a system account, first perform a search to make sure the account you want to create does not already exist.
    a. For instructions see Search System Accounts.

**NOTE:** The **Create New Account** button described below is not available until a search is performed.

2. Review the search results to see if the account you want already exists, and if not, click the **Create New Account** button that appears below the search results:




When you click **Create New Account**, the Create Account screen opens.

3. Select *System* in the **User Type** drop-down menu.

When you select user type *System*, the screen displays the fields you need to complete for a system account.

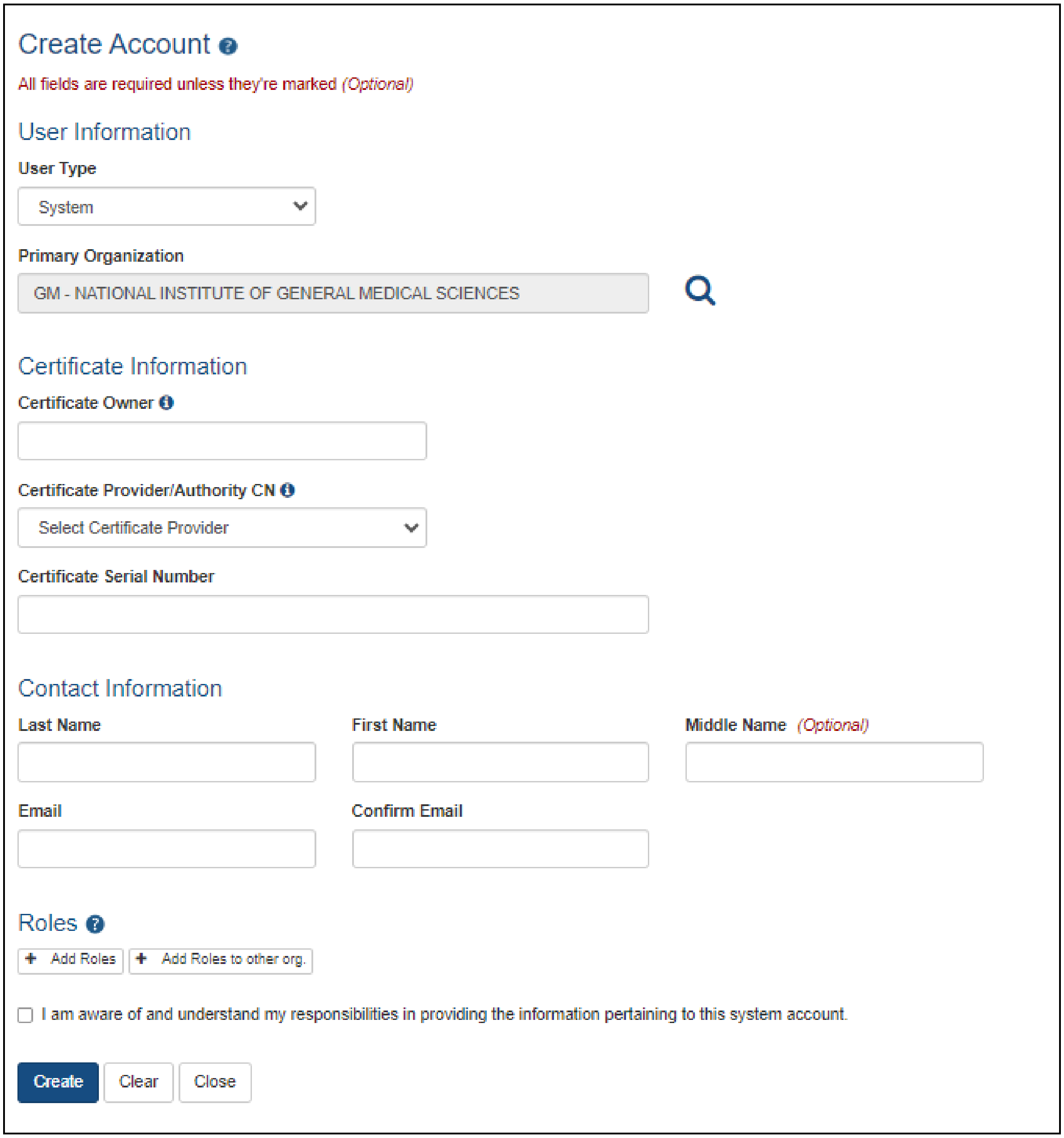



*Figure 15: Create Account Screen Displaying Creating a System Account*

4. Type in the owner in the **Certificate Owner** field. The **Certificate Owner** is the organization who acquired the certificate.
5. Select the appropriate **Certificate Provider/Authority** from the drop-down menu.

**NOTE:** Examples of the values that are available for the Certificate Provider/Authority include: Comodo, Digicert, Entrust, Geo Trust, Go Daddy, InCommon, and Thawte.

6. Enter the **Certificate Serial Number** in the format XX:XX:XX:XX:XX:XX:XX:XX.

For information on obtaining and registering a certificate from a Certificate Provider or Authority, refer to one of the Web Services Certificate (S2S) Guide:

- Section 2.4.3 for Commons users - only users with the SO role have the privileges necessary to register the certificate in AMM; Commons users must work with their SO to register their certificate

7. Complete the **Contact Information**.
8. Click the **Add Roles** button to add the roles to the account.
   a. Note the role description on the screen when adding a role.
   b. See Add System Roles for more information.
9. Select the **Agreement** checkbox below the *Roles* section.

The **Agreement** check box is mandatory for the user to acknowledge information provided for the system account. If the **Agreement** checkbox is not checked and the **Save** button is clicked, the system displays the following error message: *User must accept the agreement by checking the field*.

10. Click the **Create** button to create the account or click **Clear** to clear all fields.

When you click **Create**, the system validates the account information. If there are no errors, then the *Account Details*screen opens, displaying a success message.

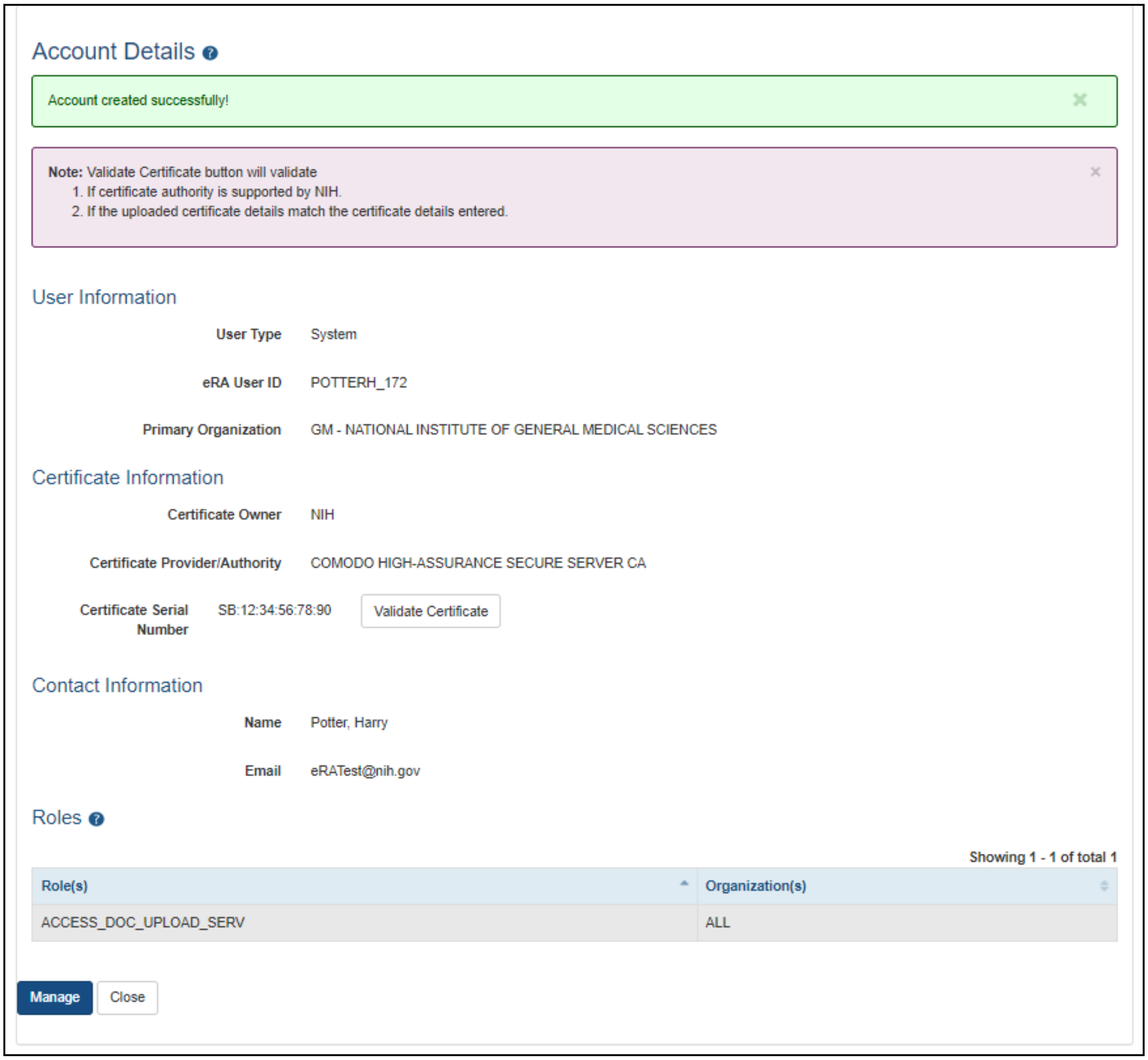



*Figure 16: Account Details screen displaying success message*

**Other Actions:**

- Click the **Validate Certificate** button to validate the certificate. See Validate Certificate for more information.
- Click the **Manage** button if you want to make additional changes. See Manage System Accounts for more information.
- Click the **Back to Search** button to return to the *Search Account* screen.

## Add System Roles

**NOTE:** The list of roles is dependent on the logged-in user's role.

1. To add system roles to the account, click on the **+ Add Roles** button on the *Create Accounts* screen.


*Figure 17: Add Roles Button on the Create Account Screen*

When the **+ Add Roles** button is clicked, the pop-up *Add Roles* screen displays.

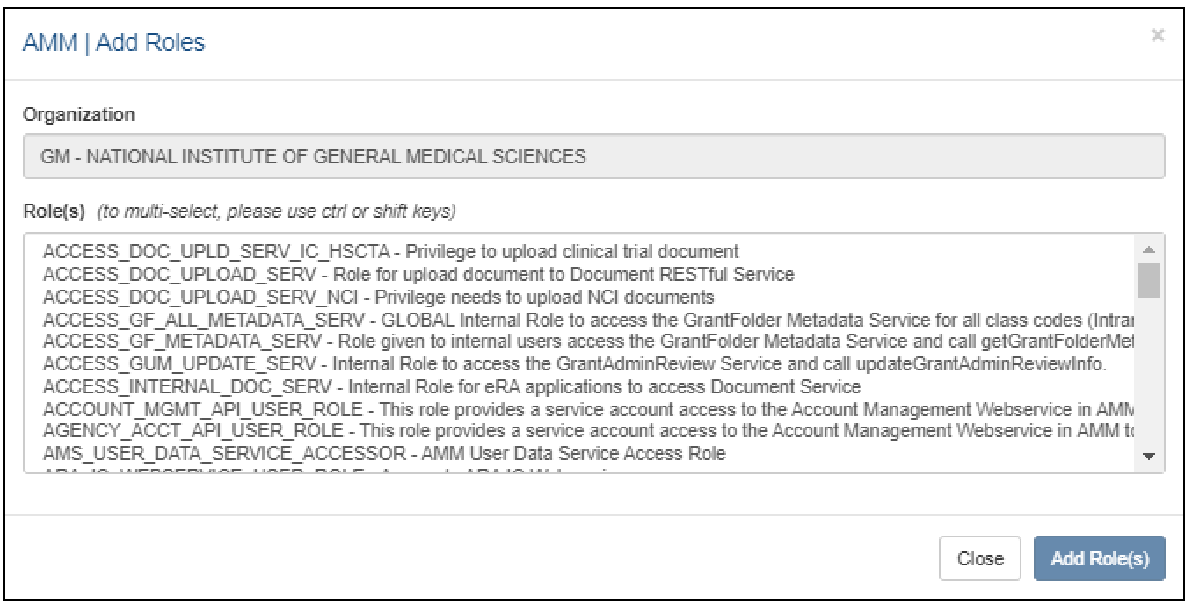



*Figure 18: Add Roles Screen Displaying Agency System Roles List*

1. Highlight the appropriate role(s).
2. Click the **Add Role(s)** button.

When the **Add Roles(s)** button is clicked, the system returns to the *Create Account* or *Manage Account* screen and displays the newly added role(s).

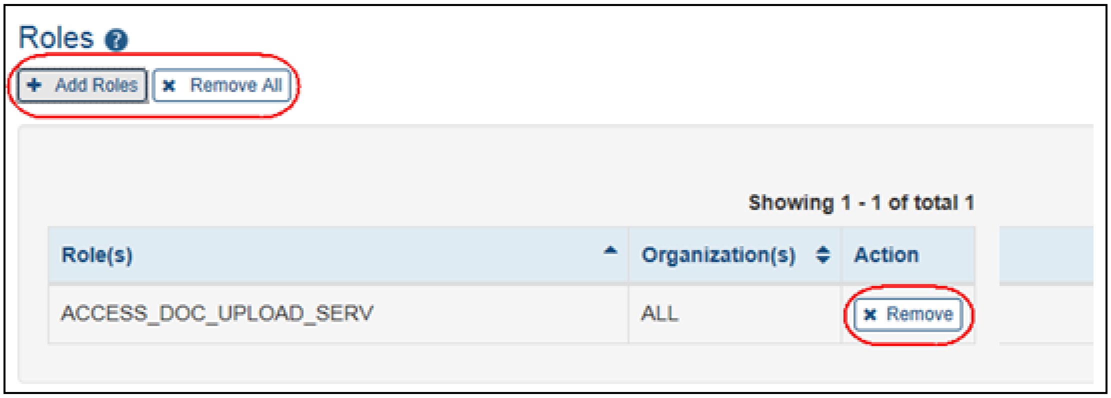



*Figure 19: Roles Section on the Create Accounts Screen for Agency Users*

3. To add additional roles, click the **+ Add Roles(s)** button. Repeat the steps above.
4. To remove a role click the appropriate **Remove** button in the **Action** column.
5. To remove all roles click the **Remove All** button.

## Add Roles to Other Org

**NOTE:** This function is available only for eRA Service Desk agents to give an account roles in another organization.

Click the **+ Add Roles to other org.** button and a pop-up search window opens so you can search for and select the other organization:


Select the other organization in this window and click **Next** to proceed to the *Add Roles* screen, as described above.

## Validate Certificate

When the **Validate Certificate** button is clicked on either the *Manage Account* or *Account Details* confirmation screen, the system displays the *AMM | Validate Certificate* screen with hyperlinks to instructions for the different browsers (i.e. Internet Explorer, Firefox, and Safari, etc.) for uploading a certificate file.

1. Perform one of the following options:
   a. To validate the certificate, click the **Validate** button on the *Validate Certificate* screen.
   b. Click the **Cancel** button to cancel the certificate validation.

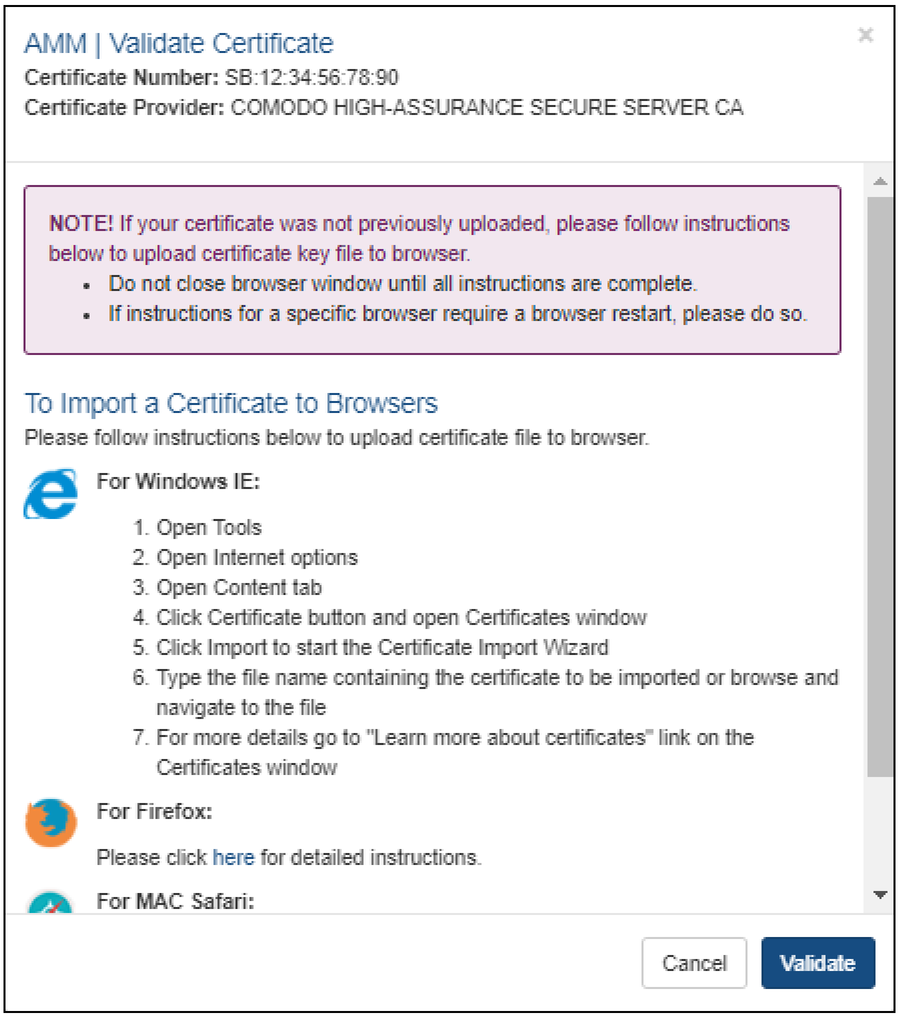



*Figure 20: Validate Certificate Screen*

When the **Validate** button is clicked, the system performs the certificate validation.

If the browser call does go through to the certificate provider, but the details of the uploaded certificate do not match the details entered in AMM, then the following warning message opens:

> Warning! - This certificate works with eRA systems correctly, but the certificate details you entered in the account do not match information in the certificate you are trying to validate. Certificate information in the account must match certificate you are trying to validate.

If there are no validation errors, a second *Validate Certificate* screen displays the following success message: Success! Your certification works with the eRA systems as expected.

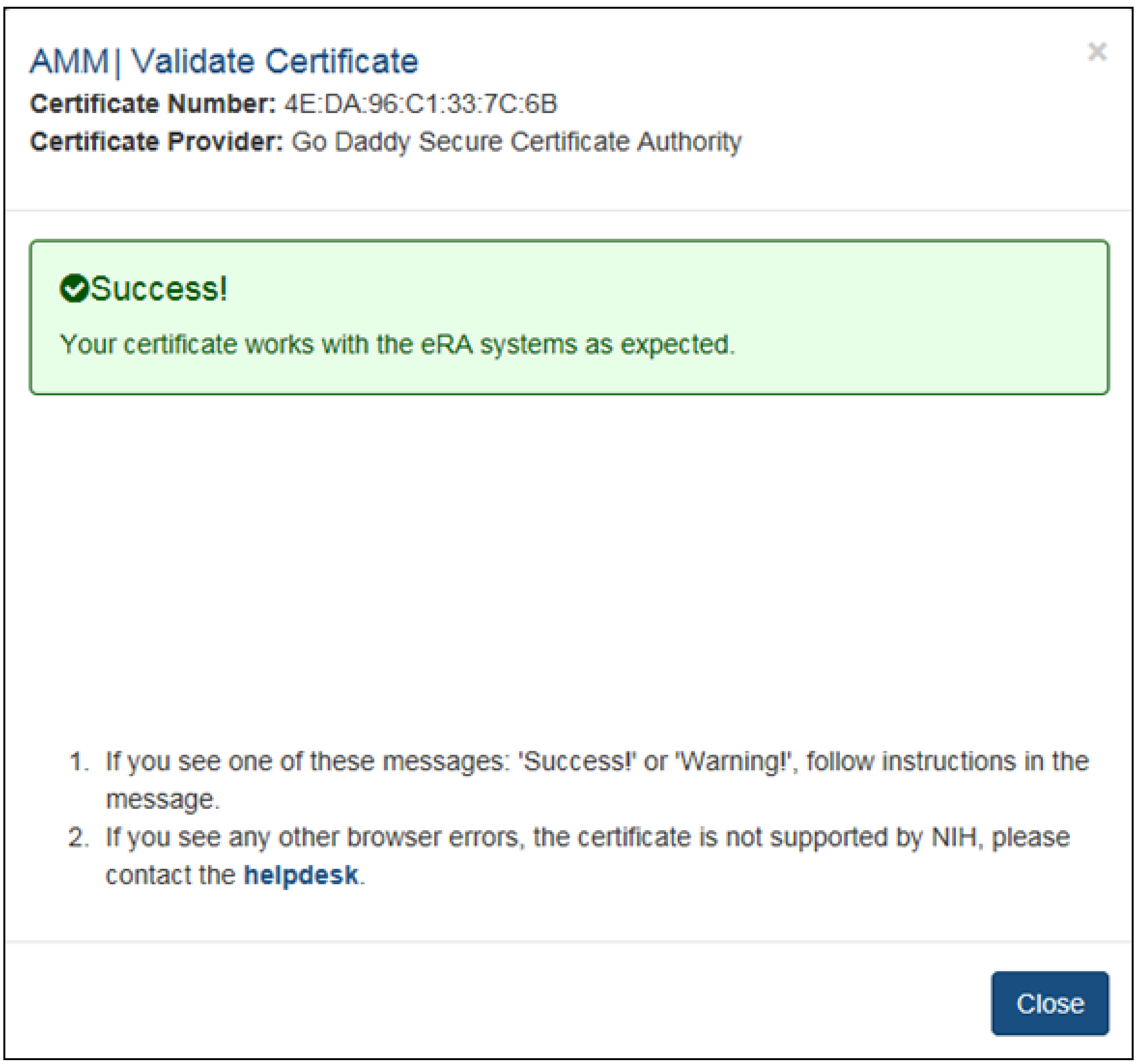


*Figure 21: Validate Certificate Screen Displaying the Success Message*

2. Click the **Close** button to close the screen.

The following audit information is audited and stored in the database:

- Certificate Number – Certificate Number of the uploaded certificate during validation
- Certificate Provider – Common Name of the uploaded certificate during validation
- Certificate Owner – The Certificate Owner that was entered during validation. The Certificate Owner is the organization who acquired the certificate.
- Time of Validation – Format: DD/MM/YYYY HH:MM:SS
- Result of Validation Attempt
  - Success
  - Validation is successful but the certificate details does not match the user entered details

# Manage Accounts

## User Accounts

Once an account is created it can be maintained via the *Manage Accounts* screen.

- Manage User Accounts

## System Accounts

Agency and Commons users can modify system accounts.

- Manage System Accounts

For information on obtaining and registering a certificate from a Certificate Provider or Authority, please refer to the Web Services Certificate (S2S) Guide:

- Section 2.4.3 for Commons users

## Managing Commons User Accounts

The following roles can manage accounts:

- Account Administrator (AA)
- Administrative Official (AO)
- Business Official (BO)
- Signing Official (SO)

1. Perform one of the following steps to manage a user account:
    a. Click the **Manage** button for an account on the *Search Accounts* screen.
    b. Click the **Manage** button on the *Account Details* screen after an account have been created or saved (edited).

Clicking the **Manage** button opens the Manage Account screen.

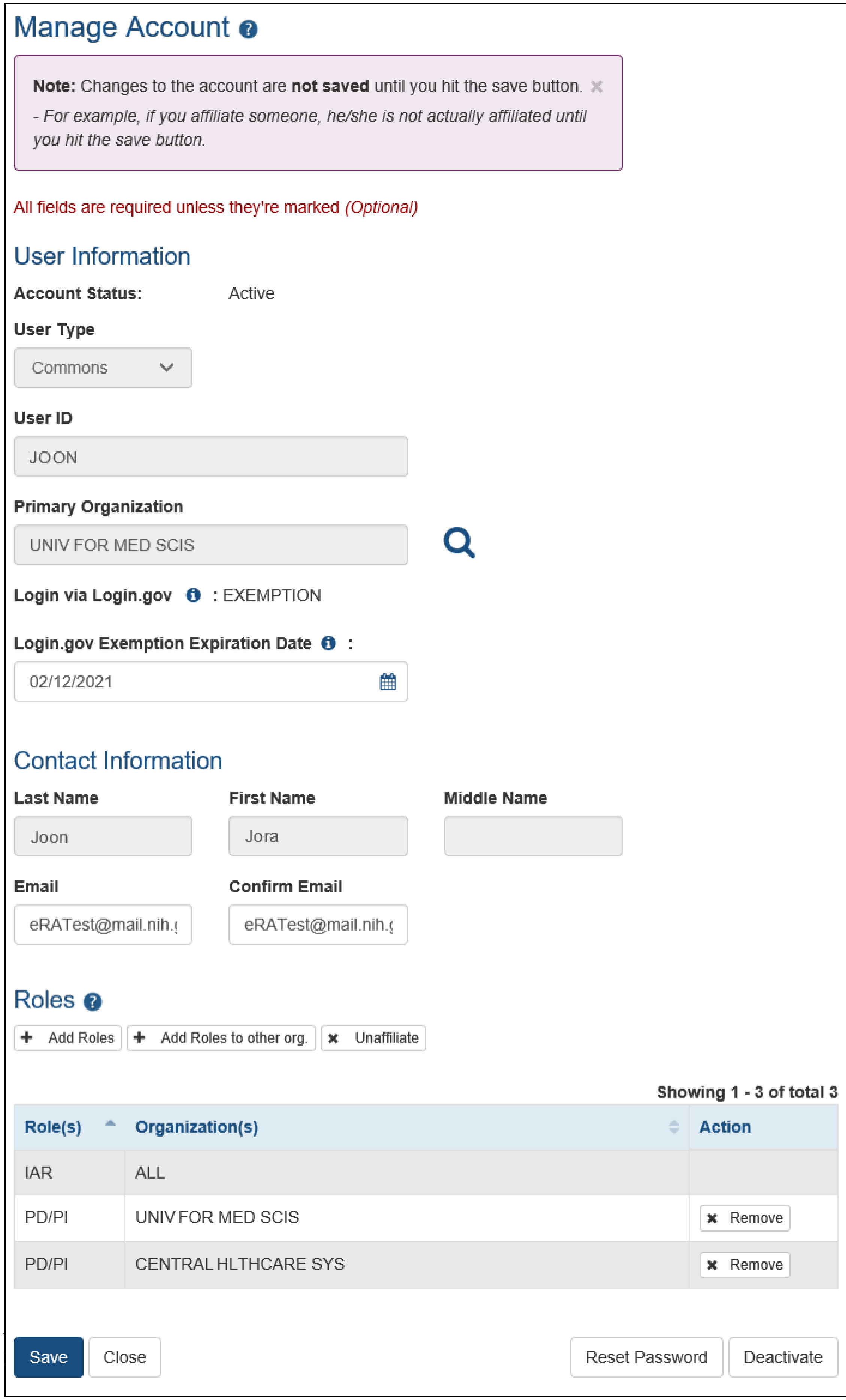

Manage Account
Note: Changes to the account are not saved until you hit the save button.
- For example, if you affiliate someone, he/she is not actually affiliated until you hit the save button.
All fields are required unless they're marked (Optional)
User Information
Account Status: Active
User Type
Commons
User ID
JOON
Primary Organization
UNIV FOR MED SCIS
Login via Login.gov : EXEMPTION
Login.gov Exemption Expiration Date :
02/12/2021
Contact Information
Last Name
Joon
First Name
Jora
Middle Name
Email
eRATest@mail.nih.g
Confirm Email
eRATest@mail.nih.g
Roles
Add Roles
Add Roles to other org.
Unaffiliate
Showing 1 - 3 of total 3
Role(s)
Organization(s)
Action
IAR
ALL
PD/PI
UNIV FOR MED SCIS
Remove
PD/PI
CENTRAL HLTHCARE SYS
Remove
Save
Close
Reset Password
Deactivate

*Figure 22: Manage Account screen for an external account*

## Actions

**You can perform these actions:**

- Edit the **Email** addresses if necessary.
- Add Roles. To add or delete roles click the **+ Add Roles** button. For more information, see Add/Delete Roles.
- To affiliate an account with an organization, click the **Affiliate** button, if displayed. (An affiliation can be created for accounts that are either not currently associated with an institution, such as an account solely with the Internet Assisted Reviewer (IAR) authority role, or for accounts that need to be associated with multiple institutions. Users with the AA or SO role may create an affiliation for their organization only. For more information, see Affiliate Account.
- If the **Unaffiliate** button is present, you can click it to unaffiliate an account. For more information, see Unaffiliate Account.
- On active accounts **Deactivate** button will be present at the bottom of the screen. Click it to Deactivate the account. For more information, see Deactivate_Reactivate Account.
- If the account has been deactivated, a **Reactivate** button will be present at the bottom of the screen. Click it to reactivate the account. For more information, see Deactivate_Reactivate Account.
- Two-Factor Authentication:

  - **Login via 2FA** — Shows the status of login.gov for this account: "Required," "Optional" or "Exemption."
    **Note:** This field is set automatically at the organization level.

  - **2FA Exemption Expiration Date** — When *Login via 2FA* is set to "Exemption," this field displays the end date for the exemption. The user can log in using eRA credentials until this date.
    **Note:** Two-factor authentication exemptions are only granted on a limited basis by the eRA Service Desk and only the eRA Service Desk can modify this date.

  - **2FA Mapping Completion Status** — Indicates whether the user's account is Mapped or Not Mapped for two-factor authentication.

### Account Statuses

AMM user accounts can have the following statuses:

- Active — A valid account in good standing.
- *Deactivated* — Account has been disabled by an administrator
- *Locked due to inactivity* — Locked by the system due to inactivity (no user activity for 120 days)
- *Pending Affiliation* — An individual account that has not been linked to an organization
- *Profile Only* — A user ID that is not associated to an account

**NOTES:**

- Administrative and reporting roles such as SO, AA, AO, FSR, etc., cannot be combined with Scientific roles such as PI, TRAINEE, ASST, etc.
- Only accounts with scientific roles such as IAR, PI, TRAINEE, POSTDOC, etc., may have multiple affiliations. If an account has any roles in addition to these, additional affiliations cannot be added.
- Fields grayed out cannot be edited.

## Add/Delete User Roles

**Agency-Specific Instructions:** State Department users only - For information on adding countries, please refer to the Add/Delete Countries topic.

**NOTE:**
1. The list of roles displayed is dependent on the logged in user's role.
2. Accounts with scientific roles should be maintained for the career of the scientist, and affiliations should be added as necessary.
3. Administrative roles cannot be combined with scientific roles on the same user account, and accounts with administrative roles cannot be affiliated with more than one institution.

1. To add user roles to an account, click on the **+ Add Roles** button at the bottom of the *Create Accounts* or *Manage Accounts* screen.


When you click **+ Add Roles**, the *Add Roles* screen opens.

**NOTE:** If you click **+ Add Roles to other org**, the Manage Account window opens first, so you can search for and select the other organization.


Select the organization and click **Next** to proceed to the *Add Roles* screen as described below.

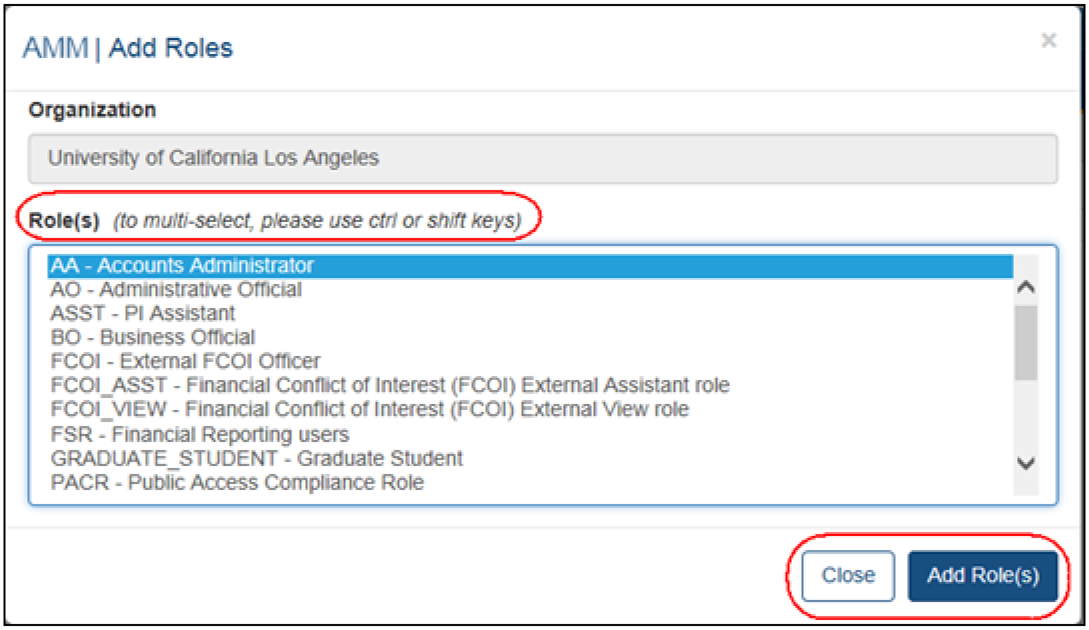



*Figure 23: Add Roles screen*

1. Scroll through the list and click to select the appropriate role(s).

   **Note**: For reference, here is a [complete list of Commons user roles](#).
2. Click the **Add Role(s)** button.

When you click **Add Roles(s)**, the system returns to the *Create Account* or *Manage Account* screen and displays the newly added role(s) .

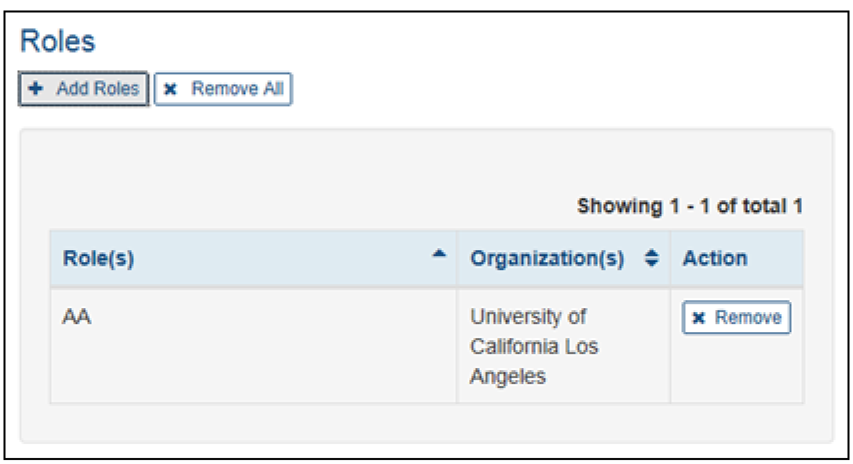



*Figure 24: Roles Section on the Create Accounts Screen*

3. To add additional roles, click the **+ Add Roles(s)** button and repeat the steps above.
4. To remove a role, click the appropriate **Remove** button in the **Action** column.
5. To remove all roles, click the **Remove All** button.

**NOTE:** You cannot remove Signing Official (SO) role when the Research Performance Progress Report (RPPR) is assigned.

**NOTE:** You cannot add user a role if the account is in deactivated status: You must reactivate the account first.

## Unaffiliate Account

1. To unaffiliate an account, click the **Unaffiliate** button in the *Roles* section of the *Manage Account* screen.

When the **Unaffiliate** button is clicked, an *Account Unaffiliation* pop-up screen displays.

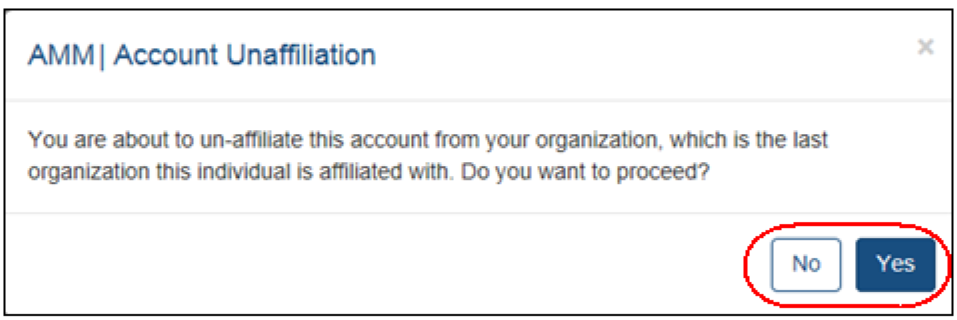



*Figure 25: Account Unaffiliation Screen*

- Click the **Yes** button to unaffiliate the account, or click **No** to cancel the unaffiliation.

After unaffiliating the account, all roles assigned to the account are removed, the account is placed in 'Pending Affiliation' status, and the **Affiliate** button appears in the *Roles* section of the *Manage Account* screen:

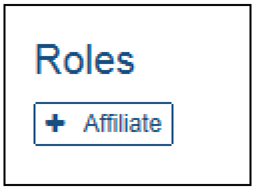



*Figure 26: Affiliate Button in Roles Section on Manage Account Screen*

**IC Transfer Process**

1. The Account Coordinator will unaffiliate the account by removing all roles for their IC.
2. The account will go into 'Pending Affiliation' Status, in which there are no roles associated with the account, and the user cannot perform any functions.
3. An Account Coordinator from the new IC will search for accounts in 'Pending Affiliation' status and select an account to affiliate.

For information on Affiliating an account, see Affiliate Account.

## Reactivate Account

Users with the following role can reactivate accounts that have been deactivated by an administrator or locked by the system due to inactivity:

- Administrative Official (AO)
- Business Official (BO)
- Signing Official (SO)

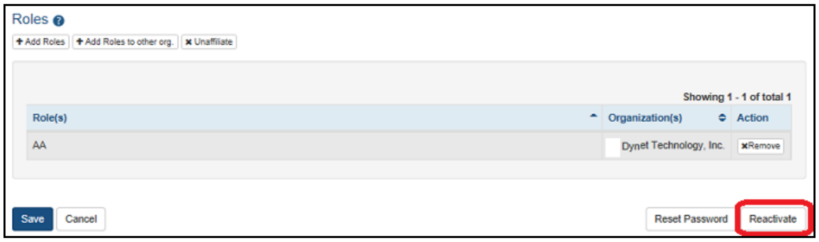
### Reactivate Account

Use these steps to reactivate an account that has been deactivated by an administrator or that has been locked due to inactivity.

**NOTE:** Commons users are required to reset their passwords after a defined time period. The system locks the account is if the user fails to rest the password. Use the Reset Password function to unlock these accounts.

1. Open the account in the *Manage Account* screen.

2. If an account is deactivated, a **Reactivate** button displays at the bottom of the *Manage Account* screen. Click this button to proceed.




3. When you click **Reactivate**, the *Reactivate Account* screen opens.

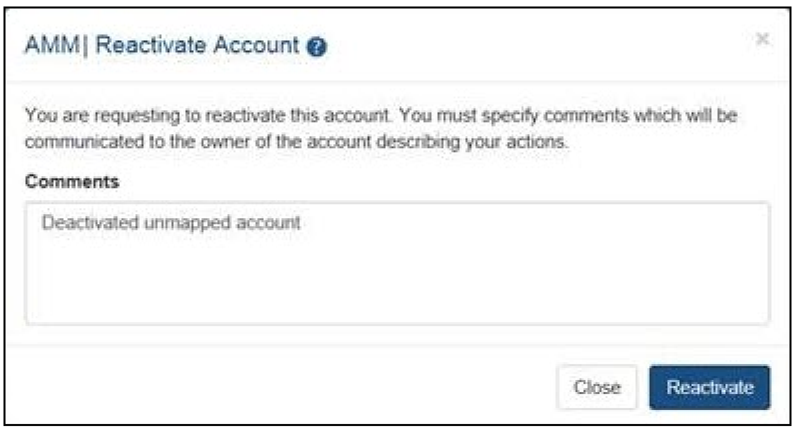



*Figure 27: Reactivate Account screen*

*Figure 28: Unlock Account screen*

4. Enter comments in the comments field to inform the user about this action (required). Click **Reactivate** to reactivate the account, or click Close to cancel.

a. Enter comments in the comments field to inform the user about this action (required).

b. Click **Reactivate** to reactivate the account, or click **Close** to cancel.

5. When you click **Reactivate**, the system reactivates the account and displays a confirmation message.
6. The account owner receives an email notification that includes the text you enter in the **Comments** field.

**NOTE:** The unlock notification asks the user to login to the account that same day. If the user does not login before the end of the day, the account is locked again.

## Manage System Accounts

System accounts are used to access eRA Web Services.

Agency and Commons users can manage system accounts in their organizations.

For information on obtaining and registering a certificate from a Certificate Provider or Authority, please refer to the Web Services Certificate (S2S) Guide:

- Section 2.4.3 for Commons users

Perform the following steps:

1. To manage a system account, first perform a search to locate the account.
   a. See Search for System Accounts for more information.
2. On the Search Results screen, click the **Manage** button for the system account you want to manage. The *Manage Account* screen opens.

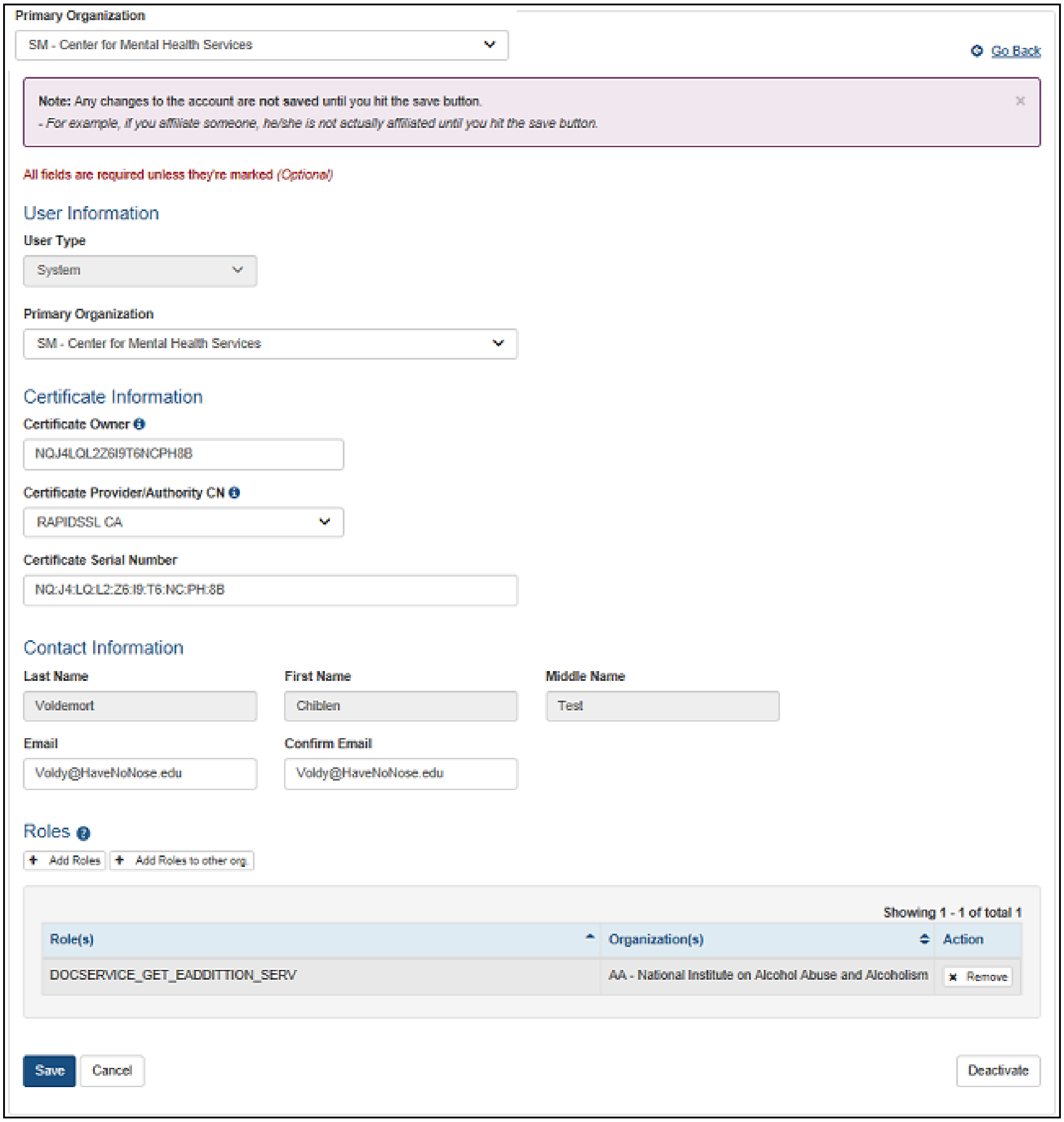



*Figure 29: Manage Account Screen for external accounts*

**NOTE:** Fields that are grayed out are not editable.

3. Edit the available fields as needed.
4. Click the **Add Roles** button to add the roles to the account. See Add System Roles for more information.
5. To remove a role, click the **Remove** button. To remove all roles, click the **Remove All** button.
6. Click **Deactivate** to deactivate an account. See Deactivate Account for more information.
7. Click **Save** to save the changes or lick **Cancel** to cancel. The *Account Details* screen opens and displays a success message.

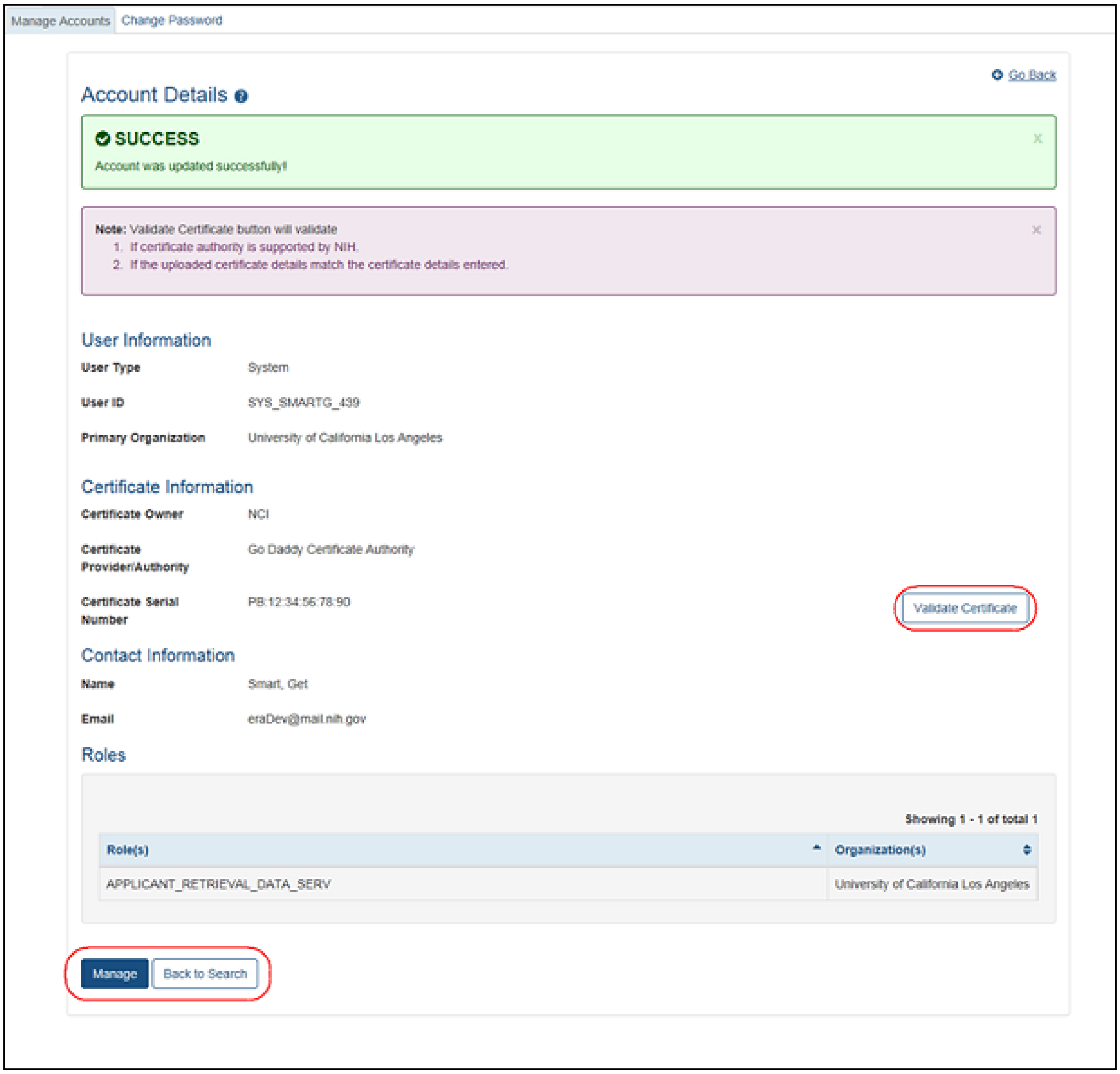



*Figure 30: Account Details Screen for external users*

8. You can perform these additional actions in the *Account Details* screen:

- If the certificate needs to be validated, click the **Validate Certificate** button. See Validate Certificate for more information.
- To return to the *Manage Accounts* screen, click the **Manage** button or the **Go Back** hyperlink.
- To return to the *Search Accounts* screen to enter new search criteria, click the **Back to Search** button.

## Add System Roles

**NOTE:** The list of roles is dependent on the logged-in user's role.

1. To add system roles to the account, click on the **+ Add Roles** button on the *Create Accounts* screen.


*Figure 31: Add Roles Button on the Create Account Screen*

When the **+ Add Roles** button is clicked, the pop-up *Add Roles* screen displays.

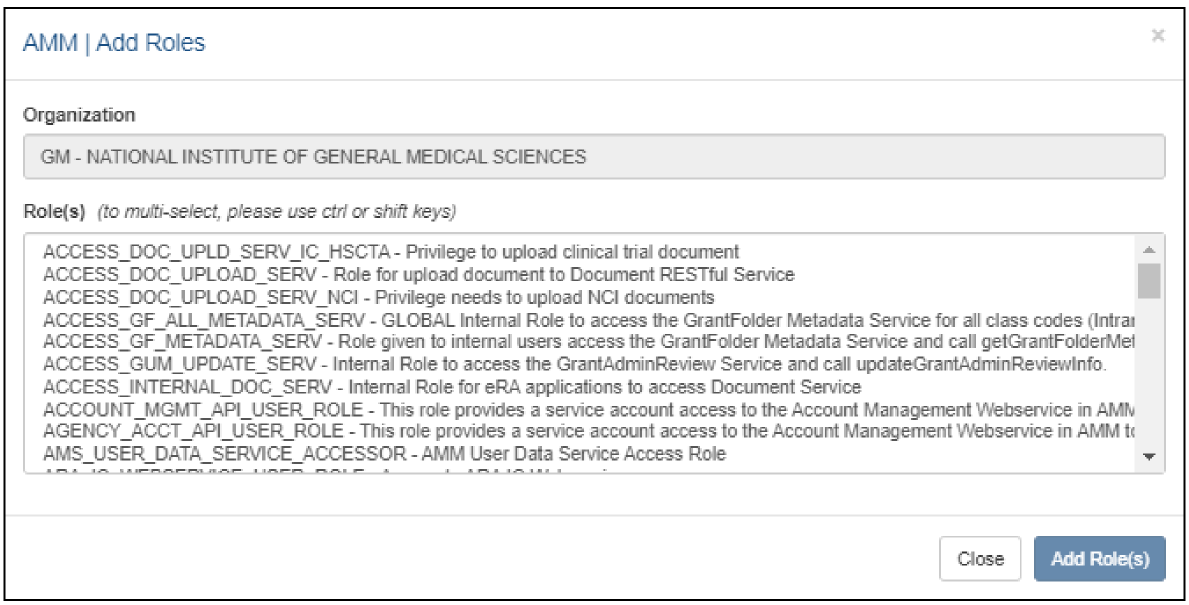



*Figure 32: Add Roles Screen Displaying Agency System Roles List*

1. Highlight the appropriate role(s).
2. Click the **Add Role(s)** button.

When the **Add Roles(s)** button is clicked, the system returns to the *Create Account* or *Manage Account* screen and displays the newly added role(s).

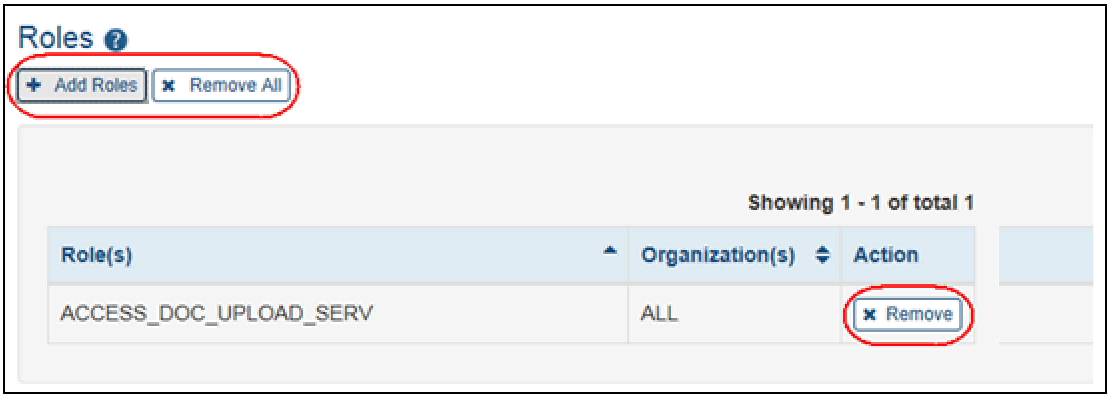



*Figure 33: Roles Section on the Create Accounts Screen for Agency Users*

3. To add additional roles, click the **+ Add Roles(s)** button. Repeat the steps above.
4. To remove a role click the appropriate **Remove** button in the **Action** column.
5. To remove all roles click the **Remove All** button.

### Add Roles to Other Org

**NOTE:** This function is available only for eRA Service Desk agents to give an account roles in another organization.

Click the **+ Add Roles to other org.** button and a pop-up search window opens so you can search for and select the other organization:


Select the other organization in this window and click **Next** to proceed to the *Add Roles* screen, as described above.

## Change Password

1. Click the **Change Password** tab:

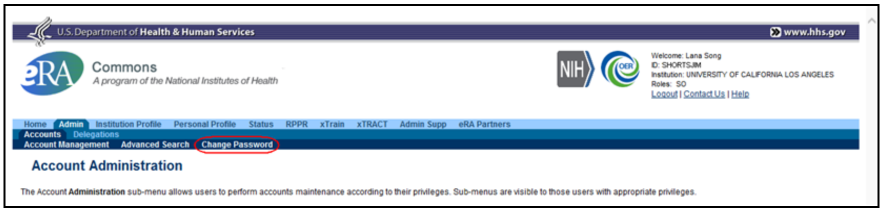



*Figure 34: Commons Menu Tabs Displaying the Change Password Tab*

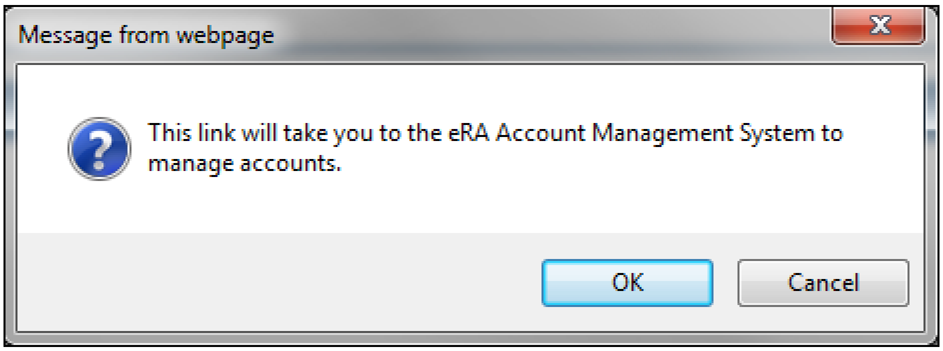



*Figure 35: Accessing AMM Pop-up Screen*

Clicking the **OK** button on the pop-up screen or the **Change Password** tab displays the *Change Password* screen in a separate browser window.

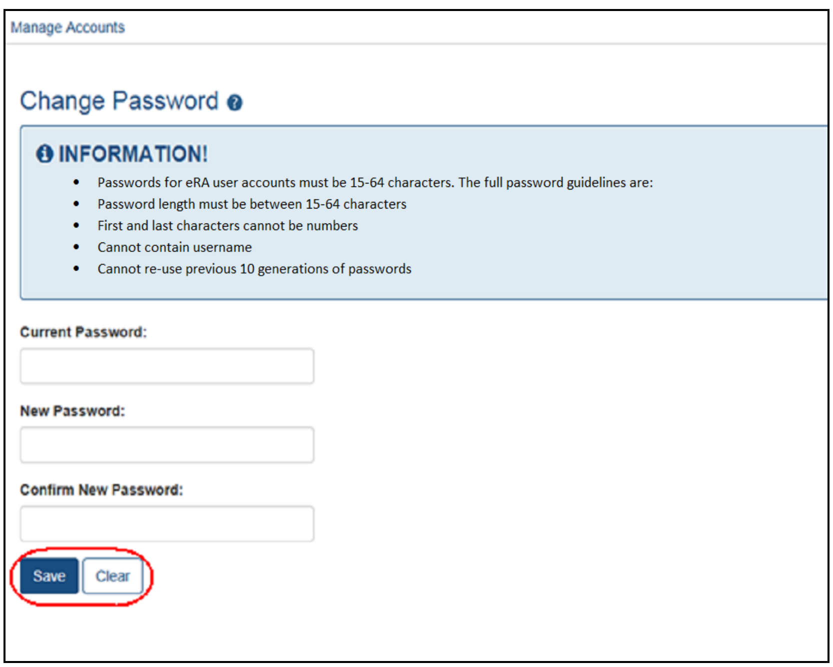


*Figure 36: Change Password Screen*

2. Enter your **Current Password**.
3. Enter a **New Password**.
4. Type your new password a second time in the **Confirm New Password** field.
5. Perform one of the following options:
    a. Click the **Save** button to save the changes.
    b. Click the **Clear** button to clear the fields.

Use your new password the next time that you log into Commons.

**NOTE:** The password guidelines are:

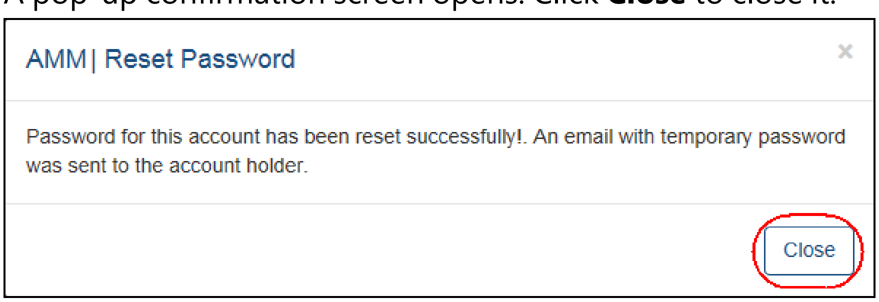
- Password length must be between 15-64 characters
- First and last characters cannot be numbers
- Cannot contain username
- Cannot re-use previous 10 generations of passwords

## Reset Password

**NOTE:** Users are required to reset their passwords after a defined time period. The system locks the account is if the user fails to reset the password. Use this procedure to unlock these accounts.

1. To reset a user's account password, open account in the the *Manage Accounts* screen and click the **Reset Password** button 

located on the lower right side of the screen.
2. A pop-up confirmation screen opens. Click **Close** to close it.



3. When you complete the password reset, an email notification with a temporary password is sent to the account holder.

# User Reports

AMM includes the following reports capabilities:

- **All Users Report** — Information on all user accounts in your organization.
- **Inactive Users Report** — Lists user accounts that have been locked due to inactivity (**note**: for internal users only)
- **Deactivated Users Report** — Lists user accounts that have been deactivated by an administrator. **Note**: For internal users only.
- **Role Description Report** — Lists all roles, role descriptions, and associated privileges for any business area. **Note**: for internal users only.

To open the reporting functions, click the **AMM User Reports** tab.

The *All Users Report* screen opens. There are two versions of this screen, as shown below. The version you see depends on the organization you belong to.

---

**TIP:** To select multiple organizations, roles, or business areas, hold the <Ctrl> key as you click.

---

## All Users Report Screen for External Users

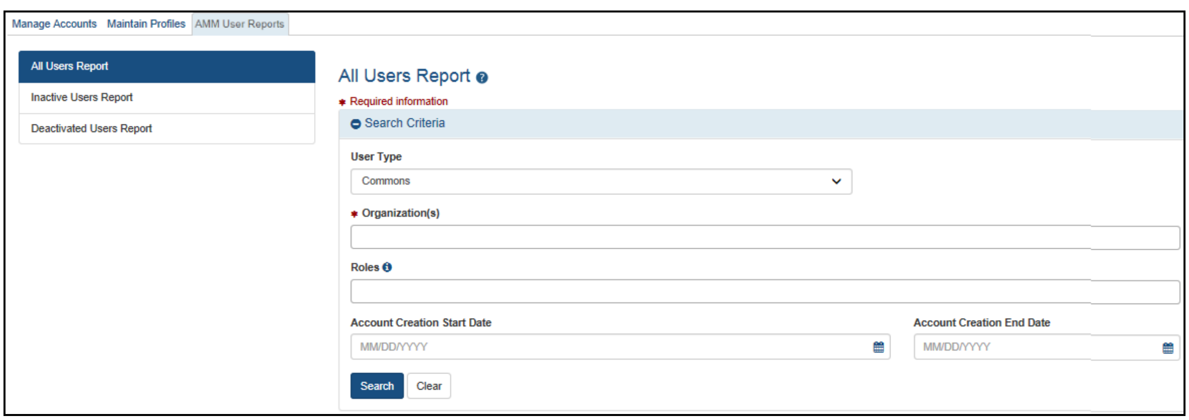



*Figure 37: All Users Report Screen for External Users*

Use this screen to run an All Users Report on external users. The **All Users Report** button is selected by default. Follow the steps below to launch the report.


1. Select "Commons" in the **User Type** field and set the search criteria in the other fields as follows:

2. **Organization** — This field displays your organization name. Service Desk agents, to select an organization, begin typing its name or ID number in this field. The live search function displays organization names as you type. When the one you want appears, scroll down and click to select it.

**NOTE:** This field is mandatory.

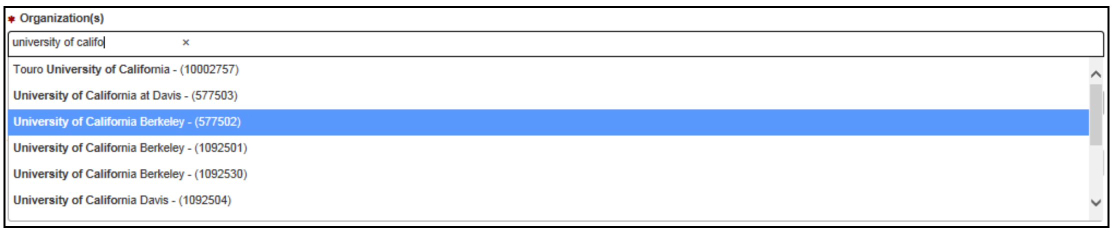



*Figure 38: Organization field, external*

3. **Roles** — Leave this field blank to report all user roles. To limit the report to one or more user roles, click this field to open the drop-down menu or begin typing the name of a role. The live search function displays roles as you type. When the one you want appears, scroll down and click to select it, as shown below.

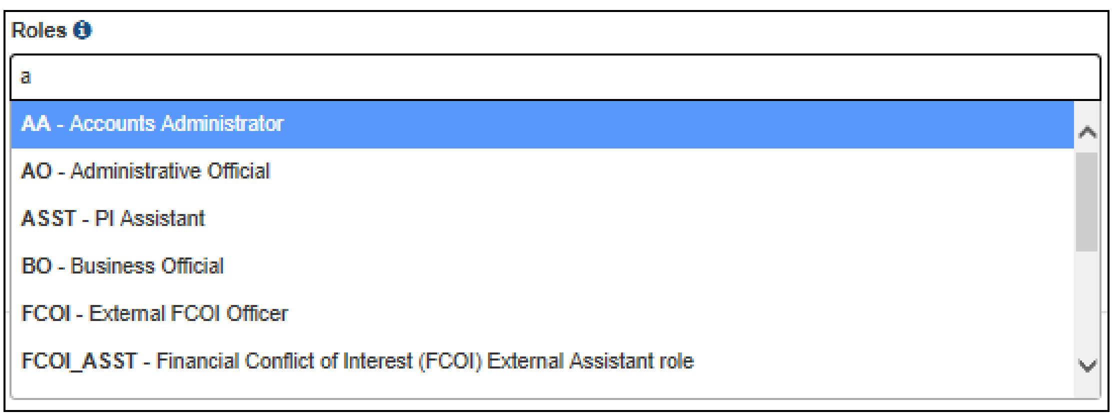



*Figure 39: Roles drop-down menu*

4. **Account Creation Start Date/End Date** — Leave these fields blank to report all time periods. To limit the report to a certain time period, enter a start date, end date, or start and end dates. Enter dates in MM/DD/YYYY format or click the calendar icon to select them from the calendar.
5. When you finish entering search criteria, click **Search** to run the report. See Report Output below.

*Figure 40: All Users Report Screen for Internal Users*

*Figure 41: All Users Report button*

*Figure 42: Organization field, internal*

*Figure 43: Business Area field*

*Figure 44: Roles field*

*Figure 45: Inactive Users Report button*

## Role Description Report

*Figure 46: Role Description Report button*

## Report Output

### All Users Report Output

Click the **All Users report** button and enter search criteria as described above to run the report. When you click the **Search** button for the All Users report, the report output displays.

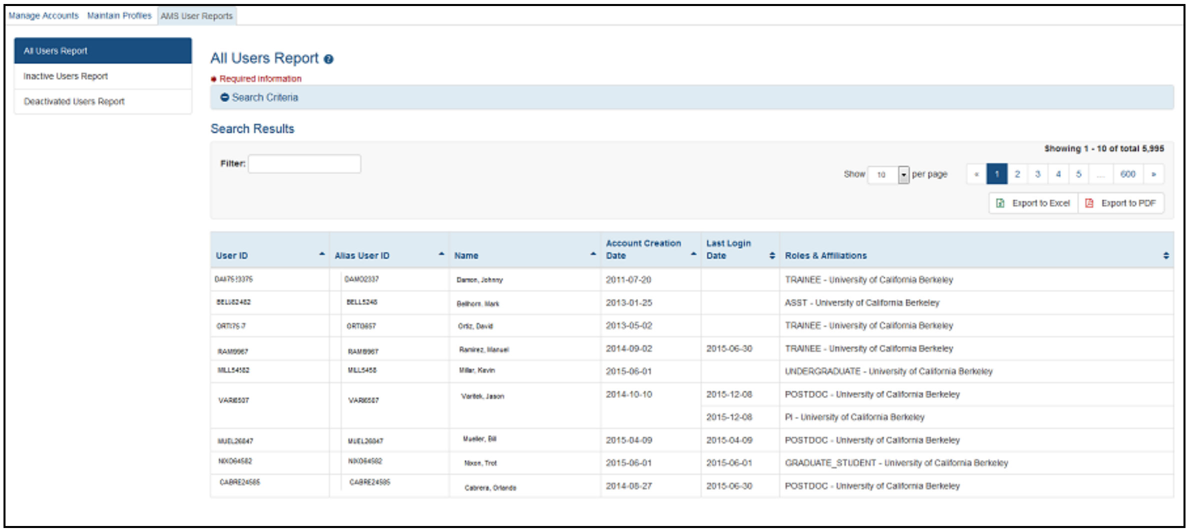



*Figure 47: All Users Report output*

*Figure 48: All Users Report output for internal users*

*Figure 49: Inactive Users Report output*

*Figure 50: Deactivated Users Report output*

## Role Description Report Output

*Figure 51: Role Description Report output*

## Navigating the Report Output

These tips for browsing, filtering and exporting the report output apply to all report types.

The report output displays include several control options:.

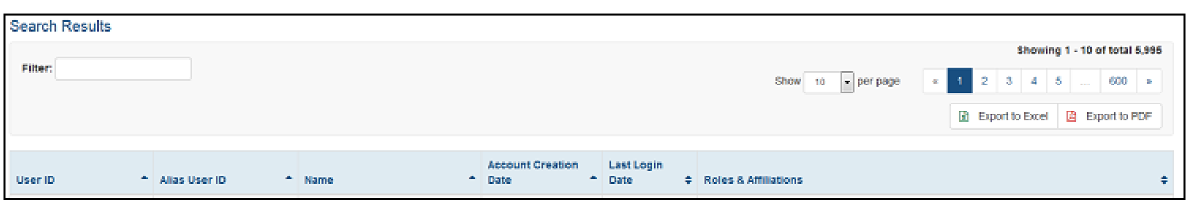
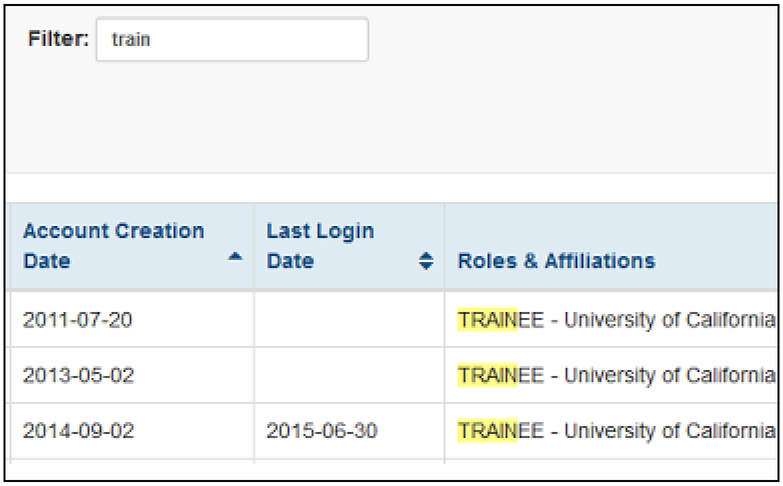



*Figure 52: Report output controls*

- To filter the report, type some text in the **Filter** field, such as a name. Only rows that contain the filter term will be displayed, and all instances of the filter text will be highlighted in yellow:




| Account Creation Date | Last Login Date | Roles & Affiliations |
|---|---|---|
| 2011-07-20 | | TRAINEE - University of California |
| 2013-05-02 | | TRAINEE - University of California |
| 2014-09-02 | 2015-06-30 | TRAINEE - University of California |

*Figure 53: Filter results*

- To adjust the number of records displayed, select a number in the **Show per page** drop-down menu.
- To navigate the report pages, click a **Page Number** or use the left and right arrow buttons.
- To re-sort the report columns in ascending or descending order, click the up/down arrows in the column headers.
- To export the report output as an Excel spreadsheet or PDF, click the appropriate **Export** button:


*Figure 54: Export button*

- **Export to Excel** — When you click this button, an open-or-save dialog opens.
    - Click **Open** to open the report data in Excel. A new Excel window opens Go to it and click the **Enable Editing** button in the yellow bar at the top of the worksheet, then work with the spreadsheet as usual.

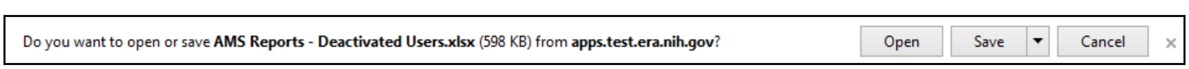


*Figure 55: Open-or-save dialog*

- **Export to PDF** — Click this button to save the report as a PDF file. A save dialog opens. Choose a location and save the file.